SYSTEMS AND METHODS FOR MANAGING AND DETECTING FRAUD IN IMAGE DATABASES USED WITH IDENTIFICATION DOCUMENTS

Priority Claim

[01] This application claims priority to the following U.S. Provisional patent application:

- Systems and Methods for Managing and Detecting Fraud in Image Databases Used With Identification Documents (Application No. 60/429,501, Attorney Docket No. P0718D, filed November 26, 2002.

Related Application Data

[02] This application also is related to the following U.S. provisional and nonprovisional patent applications:

- Integrating and Enhancing Searching of Media Content and Biometric Databases (Application No. 60/451,840, filed March 3, 2003; and
- Systems and Methods for Detecting Skin, Eye Region, and Pupils (Application No. 60/480,257, Attorney Docket No. P0845D, filed June 20, 2003).
- Identification Card Printed With Jet Inks and Systems and Methods of Making Same (Application No. 10/289,962, Attorney Docket No. P0708D, Inventors Robert Jones, Dennis Mailloux, and Daoshen Bi, filed November 6, 2002);
- Laser Engraving Methods and Compositions, and Articles Having Laser Engraving Thereon (Application No. 10/326,886, Attorney Docket No. P0724D, filed December 20, 2002—Inventors Brian Labrec and Robert Jones);
- Multiple Image Security Features for Identification Documents and Methods of Making Same (Application No. 10/325,434, Attorney Docket No. P028D, filed December 18, 2002—Inventors Brian Labrec, Joseph Anderson, Robert Jones, and Danielle Batey);
- Covert Variable Information on Identification Documents and Methods of Making Same (Application No. 10/330032, Attorney Docket No. P0732D, filed December 24, 2002 -- Inventors: Robert Jones and Daoshen Bi);
- Image Processing Techniques for Printing Identification Cards and Documents (Application No. not yet assigned, Attorney Docket No. P0819D, filed April 9, 2003—Inventors Chuck Duggan and Nelson Schneck);

- Enhanced Shadow Reduction System and Related Technologies for Digital Image capture (Application No. 60/447,502, Attorney Docket No. P0789D, filed February 13, 2003—Inventors Scott D. Haigh, Tuan A. Hoang, Charles R. Duggan, David Bohaker, and Leo M. Kenen);
- Enhanced Shadow Reduction System and Related Technologies for Digital Image capture (Application No. 10/663,439, Attorney Docket No. P0883D, filed September 15, 2003—Inventors Scott D. Haigh, Tuan A. Hoang, Charles R. Duggan, David Bohaker, and Leo M. Kenen);
- All In One Capture station for Creating Identification Documents (Application no. 10/676,362, Attorney Docket No. P0885D, filed September 30, 2003);,
- Systems and Methods for Recognition of Individuals Using Multiple Biometric Searches (Application No. 10/686,005, Attorney Docket No. P0900D—Inventors James V. Howard and Francis Frazier); and
- Detecting Skin, Eye Region, and Pupils in the Presence of Eyeglasses (Application No. not yet assigned, Attorney Docket No. P0903D—Inventor Kyungtae Hwang), filed October 23, 2003.

[03] The present invention is also related to U.S. Patent Application Nos. 09/747,735, filed December 22, 2000, 09/602,313, filed June 23, 2000, and 10/094,593, filed March 6, 2002, U.S. Provisional Patent Application No. 60/358,321, filed February 19, 2002, as well as U.S. Patent No. 6,066,594.

Technical Field

[04] Embodiments of the invention generally relate to devices, systems, and methods for data processes. More particularly, embodiments of the invention relates to systems and methods for improving the searching accuracy, use, and management of databases containing biometric information relating to individuals and for improving the accuracy of facial recognition processing.

Background and Summary of the Invention

[05] Identity theft and other related fraudulent identification activity has the potential to become a major problem to the economy, safety and stability of the United States. Identity theft refers to one individual fraudulently assuming the identity of another and may include activities such as opening credit cards in the name of another, obtaining loans, obtaining identification

documents (e.g., drivers licenses, passports), obtaining entitlement/benefits cards (e.g., Social Security Cards, welfare cards, etc.), and the like. Often, these activities are performed without the consent or knowledge of the victim. Other fraudulent identification activity can also be problematic. An individual may, for example, use either his or her "real" identity to obtain a document, such as an identification card, but may further obtain additional identification cards using one or more identification credentials that belong to another and/or one or more fictitious identification credentials.

[06] For example, to obtain an identification document such as a drivers license, a given individual may attempt to obtain multiple drivers licenses under different identities, may attempt to obtain a drivers license using false (e.g., "made up"), identification information, or may attempt to assume the identity of another to obtain a drivers license in that individual's name. In addition, individuals may alter legitimate identification documents to contain fraudulent information and may create wholly false identification documents that purport to be genuine documents.

[07] It is extremely time consuming and expensive to apprehend and prosecute those responsible for identity theft and identity fraud. Thus, to help reduce identity theft and identity fraud, it may be advisable for issuers of identity-bearing documents to take affirmative preventative steps at the time of issuance of the identity documents. Because of the large number of documents that are issued every day and the large history of already issued documents, however, it is difficult for individual employees of the issuers to conduct effective searches at the time such documents are issued (or re-issued). In addition, the complexity and amount of the information stored often precludes manual searching, at least as a starting point.

[08] For example, many government and business organizations, such as motor vehicle registries, store large databases of information about individuals. A motor vehicle registry database record may include information such as an operator's name, address, birth date, height, weight, and the like. Some motor vehicle registry databases also include images of the operator, such as a facial image and/or a fingerprint image. Unless the database is fairly small, it is nearly impossible for it to be searched manually.

[09] In some databases, part or all of the database record is digitally encoded, which helps to make it possible to perform automated searches on the database. The databases themselves, however, can still be so large that automated searching is time consuming and error prone. For

example, some states do not delete "old" images taken of a given individual. Each database record might be associated with a plurality of images. Thus, a database that contains records for 10 million individuals, could, in fact, contain 50-100 million images. If a given motor vehicle registry uses both facial and fingerprint images, the total number of images may be doubled still.

[10] One promising search technique that can be used to perform automated searching of information and which may help to reduce identity theft and identity fraud is the use of biometric authentication and/or identification systems. Biometrics is a science that refers to technologies that can be used to measure and analyze physiological characteristics, such as eye retinas and irises, facial patterns, hand geometry, and fingerprints. Some biometrics technologies involve measurement and analysis of behavioral characteristics, such as voice patterns, signatures, and typing patterns. Because biometrics, especially physiological-based technologies, measures qualities that an individual usually cannot change, it can be especially effective for authentication and identification purposes.

[11] Commercial manufacturers, such as Identix Corp of Minnetonka, Minnesota manufacture biometric recognition systems that can be adapted to be capable of comparing two images. For example, the IDENTIX FACE IT product may be used to compare two facial images to determine whether the two images belong to the same person. Other commercial products are available that can compare two fingerprint images and determine whether the two images belong to the same person. For example, U.S. Patents No 6072894, 6111517, 6185316, 5224173, 5450504, and 5991429 further describe various types of biometrics systems, including facial recognition systems and fingerprint recognition systems.

[12] Some face recognition applications use a camera to capture one or more successive images of a subject, locate the subject's face in each image, and match the subject's face to a one or faces stored in a database of stored images. In some face recognition applications, the facial images in the database of stored images are stored as processed entities called templates. A template represents the preprocessing of an image (e.g., a facial image) to a predetermined machine readable format. Encoding the image as a template helps enable automated comparison between images. For example, in a given application, a video camera can capture the image of a given subject, perform processing necessary to convert the image to a template, then compare the template of the given subject to one or more stored templates in a database, to determine if the template of the subject can be matched to one or more stored templates.

[13] Facial recognition has been deployed for applications such as surveillance and identity verification. In surveillance, for example, a given facial recognition system may be used to capture multiple images of a subject, create one or more templates based on these captured images, and compare the templates to a relatively limited "watch list" (e.g., set of stored templates), to determine if the subject's template matches any of the stored templates. In surveillance systems, outside human intervention may be needed at the time of enrolling the initial image for storage in the database, to evaluate each subject's image as it is captured and to assist the image capture process. Outside human intervention also may be needed during surveillance if a "match" is found between the template of a subject being screened and one or more of the stored templates.

[14] For example, some driver license systems include a large number of single images of individuals collected by so called "capture stations." When configured for face recognition applications, these identification systems build template databases by processing each of the individual images collect at a capture station to provide a face recognition template thereby creating a template for every individual. A typical driver license system can include millions of images. The face recognition template databases are used to detect individuals attempting to obtain multiple licenses. Another application provides law enforcement agencies with an investigative tool. The recognition database can discover other identities of a known criminal or may help identify an unidentified decedent.

[15] One difficulty in adapting commercial biometric systems to databases such as motor vehicle databases is the very large number of images that may be stored in the database. Some types of biometrics technologies can produce high numbers of false positives (falsely identifying a match between a first image and one or more other images) when the database size is very large. High numbers of false positives are sometimes seen with large databases of facial images that are used with facial recognition systems.

[16] Another potential problem with searching large databases of biometric images can be the processing delays that can accompany so-called "one to many" searches (comparing a probe image with an "unidentified" image, such as a face or finger image presented for authentication, to a large database of previously enrolled "known" images. In addition, the "many" part of "one-to-many" can vary depending on the application and/or the biometric being used. In some types of applications (such as surveillance, terrorist watch lists, authentication for admission to a facility), the "many" can be as few as a few hundred individuals, whereas for other applications

(e.g., issuance of security documents, such as passports, drivers licenses, etc.), the "many" can be many millions of images.

[17] Because many known facial recognition systems are used for surveillance applications, these facial recognition systems are optimized to work with surveillance conditions, including working with databases having relatively small numbers of templates of images (e.g., fewer than 1 million records). In addition, some facial recognition applications are able to processes multiple images captures of the same subject and, as noted previously may have an outside operator assist in initial capture of the images.

[18] For some applications, however, the optimization of the facial recognition system may be less than ideal. For example, systems such as drivers license databases may contain far more images in their databases a given surveillance application. The databases of drivers license images maintained by the Department of Motor Vehicles (DMV) in some states range from a few million records to more than 80 million records. In some instances, the DMV databases grow larger every day, because at least some DMVs do not delete any customer images, even those of deceased license holders. Another possible complication with some DMV databases is that, during the license renewal cycle, duplicate images may be created of the same person. In some instances, it may be rare to see more than two images of the same person in a DMV database, however.

[19] Still another complication with applying facial recognition processing to at least some DMV databases is the lack of operator intervention during image capture . It is time consuming, expensive, and often impossible to re-enroll the "legacy" database of DMV images so that the images are optimized for automated facial recognition.

[20] To address at least some of these and other problems, we have developed systems and methods for performing automated biometric searching of databases of captured images, where the databases can be very large in size. These systems and methods can be used during the creation and maintenance of the database as well as during the search of the database. In one embodiment, we provide a browser based system with an operator friendly interface that enables the operator to search a database of captured images for matches to a given so-called "probe" image. When matches are detected, if the operator determines that fraud or other issues may exist, the operator can add an indicator to the image and/or the image file so that future investigators are aware that issues may exist with the image. In an application such as a DMV,

the DMV can use the systems and methods of the invention to prevent the issuance of a driver's license if fraud is detected and/or to track down whether a driver's license already issued was issued based on fraudulent information and/or images.

[21] At least some systems and methods of the embodiments of the invention described herein also may help to detect patterns of fraud, geographically locate entities (including individuals, organizations, terrorist groups, etc.) committing and/or attempting to commit fraud, and help to prevent fraud.

[22] In one embodiment, the invention employs a facial recognition technique that is based on local feature analysis (LFA), such as is provided in the Identix FACE IT product.

[23] In one embodiment, we provide a system for issuing identification documents to a plurality of individuals, comprising a first database, a first server, and a workstation. The first database stores a plurality of digitized images, each digitized image comprising a biometric image of an individual seeking an identification document. The first server is in operable communication with the first database and is programmed to send, at a predetermined time, one or more digitized images from the first database to a biometric recognition system, the biometric recognition system in operable communication with a second database, the second database containing biometric templates associated with individuals whose images have been previously captured, and to receive from the biometric recognition system, for each digitized image sent, an indicator, based on the biometric searching of the second database, as to whether the second database contains any images of individuals who may at least partially resemble the digitized image that was sent. The a workstation is in operable communication with the first server and is configured to permit a user to review the indicator and to make a determination as to whether the individual is authorized to be issued an identification document or to keep an identification document in the individual's possession.

[24] The digitized image can, for example, be at least one of a facial, fingerprint, thumbprint, and iris image. The identification document can, for example, be a driver's license.

[25] The biometric recognition system can be programmed to create a biometric template based on the digitized image received from the first server and to use that biometric template to search the second database. The first server can be programmed to create a biometric template and provide that template to the biometric recognition system.

[26] The indicator can comprise a user interface the user interface retrieving from the third database the images of at least a portion of the images of individuals that the biometric recognition system has determined may at least partially resemble the digitized image that was sent. In at least one embodiment, the user interface is operable to permit a user to do at least one of the following functions:

visually compare the digitized image that was sent directly to an image of an individual whose data was returned in the indicator by the facial recognition search system;

visually compare demographic information associated with the individual whose digitized image was sent directly to demographic information of an individual whose data was returned in the indicator by the facial recognition search system;;

visually compare the other biometric information associated with the digitized image that was sent to other biometric information associated with an individual whose data was returned in the indicator by the facial recognition search system;

create a new biometric template of the digitized image that was sent and conduct a new search of the biometric recognition search system using the new biometric template;

perform a re-alignment of the digitized image and use the re-alignment data to conduct a new search of the biometric recognition search system;

capture a new image of the individual whose digitized image was sent;

adding a notification to a record associated with at least one of the digitized image that was sent and the data that was returned in the indicator by the biometric recognition search system, the notification providing an alert that there may be a problem with the record; and

selecting at least one of the images of an individual whose data was returned in the indicator by the facial recognition search system and sending that image to the biometric recognition search system to run a search on that image.

[27] In one embodiment, we provide a method for screening a plurality of applicants each seeking to be issued an identification document, comprising:

(a) storing a digitized image of each applicant in a first database;

(b) providing a predetermined portion of the images in the first database, at a predetermined time, to a biometric searching system, the biometric searching system comparing the digitized image of each applicant to a plurality of previously captured images of individuals stored in a third database and returning to a second database, for each applicant, an result containing a list of matches to each image, each match having a score;

(c) selecting from the second database those results having a score above a

predetermined threshold and providing the results to a fourth database;

(d) providing the selected results to an investigator; and

(e) displaying to the investigator, upon request, information about each selected result.

[28] The method can also include the steps of receiving a notification from the investigator relating to at least one of the results, and adding a notification to a record associated with the corresponding result, the notification remaining in the record until removed by an authorized individual and being visible to other investigators until removed.

[29] In another embodiment we provide a computer implemented method of creating a biometric template of an individual for facial recognition processing, comprising:

sending an image of the individual to a plurality of eye finding modules, each eye finding module configured to find the location of at least one eye of the individual in the image;

receiving locations of the at least one eye from each respective eye finding module in the plurality of eye finding modules; and

applying at least one rule to the received locations to determine the eye location to be used for creation of the biometric template.

[30] In one embodiment, the predetermined rule can comprise at least one or more of the following rules;

selecting as an eye location the average of the received eye locations;

selecting as an eye location a weighted average of the received eye locations;

selecting as an eye location the location that is closest to the eye location determined by a majority of the plurality of eye finding modules;

removing from the received eye locations any eye locations that are outside of a predetermined boundary;

selecting as an eye location an eye location that is the center of gravity of the received eye locations;

removing from the received eye locations any eye locations that do not fit known eye characteristics, and

removing from the received eye locations any eye locations that are not within a predetermined distance or slope from the eye locations of the other eye of the individual

[31] In one embodiment, we provide a method of searching a database of biometric templates, each biometric template associated with a corresponding facial image of an individual, for an image of an individual who substantially resembles an individual in a probe image, comprising:

receiving a probe image of an individual at a client;

determining the eye locations of the individual;

applying a predetermined rule to determine if the eye locations are acceptable;

if the eye locations are acceptable, creating a probe biometric template using the eye locations; and

searching a database of biometric templates using the probe biometric template.

[32] In another embodiment we provide a system for investigating an image of an individual, comprising:

a first database, the first database storing at least one digitized image, the digitized image comprising a biometric image of an individual seeking an identification document;

a second database, the second database storing a plurality of digitized images of individuals whose images have been previously captured;

means for determining whether any of the images in the second database match any of the images in the first database to a predetermined degree and for providing such matches an investigator, the means for determining being in operable communication with the first and second databases; and

means for allowing the investigator to compare information associated with the first digitized image with information associated with any of the matches, the means for allowing being in operable communication with at least a third database capable of providing the information associated with the first digitized image and information associated with any of the matches.

[33] These and other embodiments of the invention are described below

BRIEF DESCRIPTION OF THE DRAWINGS

[34] The foregoing features of this invention, as well as the invention itself, may be more fully understood from the following description and the drawings in which:

[35] FIG. 1 is a block diagram of a computer system usable in the embodiments of the invention described herein;

[36] FIG. 2 is a block diagram of a system for biometric searching in accordance with a first embodiment of the invention;

[37] FIG. 3 is a block diagram of a system for biometric searching in accordance with a second embodiment of the invention;

[38] FIG. 4 is a block diagram of a system for biometric searching in accordance with a third embodiment of the invention;

[39] FIG. 5A is a diagram illustrating a first process for communication between a photo verification system and a facial recognition search system, in accordance with one embodiment of the invention;

[40] FIG. 5B is a diagram illustrating a second process for communication between a photo verification system and a facial recognition search system, in accordance with one embodiment of the invention;

[41] FIG. 6A is a flow chart of a first method for alignment of an image, in accordance one embodiment of the invention;

[42] FIG. 6B is a flow chart of a second method for alignment of an image, in accordance one embodiment of the invention;

[43] FIG. 7 is a flow chart of a method for conducting biometric searches at a biometric search engine, in accordance with one embodiment of the invention;

[44] FIG. 8 is a flow chart of a method for conducting biometric searches at a user workstation, in accordance with one embodiment of the invention;

[45] FIG. 9 is an illustrative example of a screen shot of a user interface showing an image that can be used as a probe image, in accordance with one embodiment of the invention;

[46] FIG. 10 is an illustrative example of a screen shot of a probe image verification list, in accordance with one embodiment of the invention;

[47] FIGs. 11A-11B are illustrative examples of probe images and returned results, respectively, for the system of any one of FIGs. 2-4;

[48] FIG. 12A-12B are illustrative examples of a side by side comparison of a probe image and a retrieved image, respectively, including demographic and biometric data, for the system of any one of FIGs. 2-4;

[49] FIG. 13 is an illustrative example of a screen shot of a candidate list screen presented to a user, in accordance with one embodiment of the invention;

[50] FIG. 14 is an illustrative example of a screen shot of a side by side comparison showing portraits and limited demographic information, in accordance with one embodiment of the invention;

[51] FIG. 15 is an illustrative example of a screen shot of a side by side comparison screen showing fingerprints and signatures, in accordance with one embodiment of the invention; and

[52] FIG. 16 is a flow chart of a process a biometric search that includes evaluation of eye locations, in accordance with one embodiment of the invention.

[53] The drawings are not necessarily to scale, emphasis instead is generally placed upon illustrating the principles of the invention. In addition, in the drawings, like reference numbers indicate like elements. Further, in the figures of this application, in some instances, a plurality of system elements or method steps may be shown as illustrative of a particular system element, and a single system element or method step may be shown as illustrative of a plurality of a particular systems elements or method steps. It should be understood that showing a plurality of a particular element or step is not intended to imply that a system or method implemented in accordance with the invention must comprise more than one of that element or step, nor is it intended by illustrating a single element or step that the invention is limited to embodiments having only a single one of that respective elements or steps. In addition, the total number of elements or steps shown for a particular system element or method is not intended to be limiting; those skilled in the art will recognize that the number of a particular system element or method steps can, in some instances, be selected to accommodate the particular user needs.

DETAILED DESCRIPTION

[54] Before describing various embodiments of the invention in detail, it is helpful to define some terms used herein and explain further some of the environments and applications in which at least some embodiments of the invention can be used.

[55] *Identification Documents*

[56] In the foregoing discussion, the use of the word "ID document" or "identification document" or "security document" is broadly defined and intended to include all types of ID documents, including (but not limited to), documents, magnetic disks, credit cards, bank cards, phone cards, stored value cards, prepaid cards, smart cards (e.g., cards that include one more semiconductor chips, such as memory devices, microprocessors, and microcontrollers), contact cards, contactless cards, proximity cards (e.g., radio frequency (RFID) cards), passports, driver's licenses, network access cards, employee badges, debit cards, security cards, visas, immigration documentation, national ID cards, citizenship cards, social security cards, security badges, certificates, identification cards or documents, voter registration and/or identification cards, police ID cards, border crossing cards, security clearance badges and cards, legal instruments, gun permits, badges, gift certificates or cards, membership cards or badges, and tags. Also, the terms "document," "card," "badge" and "documentation" are used interchangeably throughout this patent application.). In at least some aspects of the invention, ID document can include any item of value (e.g., currency, bank notes, and checks) where authenticity of the item is important and/or where counterfeiting or fraud is an issue.

[57] In addition, in the foregoing discussion, "identification" at least refers to the use of an ID document to provide identification and/or authentication of a user and/or the ID document itself. For example, in a conventional driver's license, one or more portrait images on the card are intended to show a likeness of the authorized holder of the card. For purposes of identification, at least one portrait on the card (regardless of whether or not the portrait is visible to a human eye without appropriate stimulation) preferably shows an "identification quality" likeness of the holder such that someone viewing the card can determine with reasonable confidence whether the holder of the card actually is the person whose image is on the card. "Identification quality" images, in at least one embodiment of the invention, include covert images that, when viewed using the proper facilitator (e.g., an appropriate light or temperature source), provide a discernable image that is usable for identification or authentication purposes.

[58] Further, in at least some embodiments, "identification" and "authentication" are intended to include (in addition to the conventional meanings of these words), functions such as recognition, information, decoration, and any other purpose for which an indicia can be placed upon an article in the article's raw, partially prepared, or final state. Also, instead of ID documents, the inventive techniques can be employed with product tags, product packaging, business cards, bags, charts, maps, labels, etc., etc., particularly those items including marking of an laminate or over-laminate structure. The term ID document thus is broadly defined herein to include these tags, labels, packaging, cards, etc.

[59] Many types of identification cards and documents, such as driving licenses, national or government identification cards, bank cards, credit cards, controlled access cards and smart cards, carry thereon certain items of information which relate to the identity of the bearer. Examples of such information include name, address, birth date, signature and photographic image; the cards or documents may in addition carry other variant data (i.e., data specific to a particular card or document, for example an employee number) and invariant data (i.e., data common to a large number of cards, for example the name of an employer). All of the cards described above will hereinafter be generically referred to as "ID documents".

[60] As those skilled in the art know, ID documents such as drivers licenses can contain information such as a photographic image, a bar code (which may contain information specific to the person whose image appears in the photographic image, and/or information that is the same from ID document to ID document), variable personal information, such as an address, signature, and/or birthdate, biometric information associated with the person whose image appears in the photographic image (e.g., a fingerprint), a magnetic stripe (which, for example, can be on the a side of the ID document that is opposite the side with the photographic image), and various security features, such as a security pattern (for example, a printed pattern comprising a tightly printed pattern of finely divided printed and unprinted areas in close proximity to each other, such as a fine-line printed security pattern as is used in the printing of banknote paper, stock certificates, and the like).

[61] An exemplary ID document can comprise a core layer (which can be pre-printed), such as a light-colored, opaque material (e.g., TESLIN (available from PPG Industries) or polyvinyl chloride (PVC) material). The core is laminated with a transparent material, such as clear PVC to form a so-called "card blank". Information, such as variable personal information (e.g., photographic information), is printed on the card blank using a method such as Dye Diffusion

Thermal Transfer ("D2T2") printing (described further below and also described in commonly assigned United States Patent No. 6066594, the contents of which are hereby incorporated by reference). The information can, for example, comprise an indicium or indicia, such as the invariant or nonvarying information common to a large number of identification documents, for example the name and logo of the organization issuing the documents. The information may be formed by any known process capable of forming the indicium on the specific core material used.

[62] To protect the information that is printed, an additional layer of transparent overlaminate can be coupled to the card blank and printed information, as is known by those skilled in the art. Illustrative examples of usable materials for overlaminates include biaxially oriented polyester or other optically clear durable plastic film.

[63] In the production of images useful in the field of identification documentation, it may be desirable to embody into a document (such as an ID card, drivers license, passport or the like) data or indicia representative of the document issuer (e.g., an official seal, or the name or mark of a company or educational institution) and data or indicia representative of the document bearer (e.g., a photographic likeness, name or address). Typically, a pattern, logo or other distinctive marking representative of the document issuer will serve as a means of verifying the authenticity, genuineness or valid issuance of the document. A photographic likeness or other data or indicia personal to the bearer will validate the right of access to certain facilities or the prior authorization to engage in commercial transactions and activities.

[64] Identification documents, such as ID cards, having printed background security patterns, designs or logos and identification data personal to the card bearer have been known and are described, for example, in U.S. Pat. No. 3,758,970, issued Sep. 18, 1973 to M. Annenberg; in Great Britain Pat. No. 1,472,581, issued to G. A. O. Gesellschaft Fur Automation Und Organisation mbH, published Mar. 10, 1976; in International Patent Application PCT/GB82/00150, published Nov. 25, 1982 as Publication No. WO 82/04149; in U.S. Pat. No. 4,653,775, issued Mar. 31, 1987 to T. Raphael, et al.; in U.S. Pat. No. 4,738,949, issued Apr. 19, 1988 to G. S. Sethi, et al.; and in U.S. Pat. No. 5,261,987, issued Nov. 16 1993 to J. W. Luening, et al.

[65] Commercial systems for issuing ID documents are of two main types, namely so-called "central" issue (CI), and so-called "on-the-spot" or "over-the-counter" (OTC) issue. CI type ID documents are not immediately provided to the bearer, but are later issued to the bearer from a

central location. For example, in one type of CI environment, a bearer reports to a document station where data is collected, the data are forwarded to a central location where the card is produced, and the card is forwarded to the bearer, often by mail. In contrast to CI identification documents, OTC identification documents are issued immediately to a bearer who is present at a document-issuing station. An OTC assembling process provides an ID document "on-the-spot". (An illustrative example of an OTC assembling process is a Department of Motor Vehicles ("DMV") setting where a driver's license is issued to person, on the spot, after a successful exam.). Further details relating to various methods for printing and production of identification documents can be found in the following commonly assigned patent applications, all of which are hereby incorporated by reference:

- Identification Card Printed With Jet Inks and Systems and Methods of Making Same (Application No. 10/289,962, Attorney Docket No. P0708D, Inventors Robert Jones, Dennis Mailloux, and Daoshen Bi, filed November 6, 2002);
- Laser Engraving Methods and Compositions, and Articles Having Laser Engraving Thereon (Application No. 10/326,886, Attorney Docket No. P0724D, filed December 20, 2002—Inventors Brian Labrec and Robert Jones);
- Multiple Image Security Features for Identification Documents and Methods of Making Same (Application No. 10/325,434, Attorney Docket No. P028D, filed December 18, 2002—Inventors Brian Labrec, Joseph Anderson, Robert Jones, and Danielle Batey); and
- Identification Card Printer-Assembler for Over the Counter Card Issuing (Application No. not yet assigned, Attorney Docket No. P0829D, filed May 12, 2003—Inventors Dennis Mailloux, Robert Jones, and Daoshen Bi).

[66] *Biometrics*

[67] Biometrics relates generally to the science of measuring and analyzing biological characteristics, especially those of humans. One important application of biometrics is its use in security-related applications, such as identification of an individual or authentication of an individual's identity by using measurable, individualized, and often unique, human physiological characteristics. Examples of human physiological characteristics that can be used as biometric identifiers include (but are not limited to) face, fingerprint (including use for both fingerprint recognition systems and Automated Fingerprint Identification Systems (AFIS)), thumbprint, hand print, iris, retina, hand geometry, finger geometry, thermogram (heat signatures of a given physiological feature, e.g. the face, where the image is captured using a device such as an

infrared camera and the heat signature is used to create a biometric template used for matching), hand vein (measuring the differences in subcutaneous features of the hand using infrared imaging), signature, voice, keystroke dynamic, odor, breath, and deoxyribonucleic acid (DNA). We anticipate that any one or more of these biometrics is usable with the embodiments of the invention described herein.

[68] The reader is presumed to be familiar with how each of the biometrics listed above works and how biometric templates are created with each method. We note, however, that embodiments of the invention can utilize many different types of information to create biometric templates. For example, to create face and/or finger templates, information that can be used may include (but is not limited to), law enforcement images (e.g., mug shots, fingerprint exemplars, etc.), print images from any source (e.g., photographs, video stills, etc.), digitized or scanned images, images captured at a capture station, information provided by other databases, and/or sketches (e.g., police sketches).

[69] *Detailed Description of the Figures*

[70] Systems and methods described herein in accordance with the invention can be implemented using any type of general purpose computer system, such as a personal computer (PC), laptop computer, server, workstation, personal digital assistant (PDA), mobile communications device, interconnected group of general purpose computers, and the like, running any one of a variety of operating systems. FIG. 1 is a block diagram of a computer system usable as the workstation 10 in the embodiments described herein

[71] Referring briefly to FIG. 1, the workstation 10 includes a central processor 12, associated memory 14 for storing programs and/or data, an input/output controller 16, a network interface 18, a display device 20, one or more input devices 22, a fixed or hard disk drive unit 24, a floppy disk drive unit 26, a tape drive unit 28, and a data bus 30 coupling these components to allow communication therebetween.

[72] The central processor 12 can be any type of microprocessor, such as a PENTIUM processor, made by Intel of Santa Clara, California. The display device 20 can be any type of display, such as a liquid crystal display (LCD), cathode ray tube display (CRT), light emitting diode (LED), and the like, capable of displaying, in whole or in part, the outputs generated in accordance with the systems and methods of the invention. The input device 22 can be any type

of device capable of providing the inputs described herein, such as keyboards, numeric keypads, touch screens, pointing devices, switches, styluses, and light pens. The network interface 18 can be any type of a device, card, adapter, or connector that provides the computer system 10 with network access to a computer or other device, such as a printer. In one embodiment of the present invention, the network interface 18 enables the workstation 10 to connect to a computer network such as the Internet.

[73] Those skilled in the art will appreciate that computer systems embodying the present invention need not include every element shown in FIG. 1, and that equivalents to each of the elements are intended to be included within the spirit and scope of the invention. For example, the workstation 10 need not include the tape drive 28, and may include other types of drives, such as compact disk read-only memory (CD-ROM) drives. CD-ROM drives can, for example, be used to store some or all of the databases described herein.

[74] In at least one embodiment of the invention, one or more computer programs define the operational capabilities of the workstation 10. These programs can be loaded into the computer system 10 in many ways, such as via the hard disk drive 24, the floppy disk drive 26, the tape drive 28, or the network interface 18. Alternatively, the programs can reside in a permanent memory portion (e.g., a read-only-memory (ROM)) chip) of the main memory 14. In another embodiment, the workstation 10 can include specially designed, dedicated, hard-wired electronic circuits that perform all functions described herein without the need for instructions from computer programs.

[75] In at least one embodiment of the present invention, the workstation 10 is networked to other devices, such as in a client-server or peer to peer system. For example, referring to FIG. 1, the workstation 10 can be networked with an external data system 17. The workstation 10 can, for example, be a client system, a server system, or a peer system. In one embodiment, the invention is implemented at the server side and receives and responds to requests from a client, such as a reader application running on a user computer.

[76] The client can be any entity, such as a the workstation 10, or specific components thereof (e.g., terminal, personal computer, mainframe computer, workstation, hand-held device, electronic book, personal digital assistant, peripheral, etc.), or a software program running on a computer directly or indirectly connected or connectable in any known or later-developed manner to any type of computer network, such as the Internet. For example, a representative

client is a personal computer that is x86-, PowerPC.RTM., PENTIUM-based, or RISC-based, that includes an operating system such as IBM.RTM, LINUX, OS/2.RTM. or any member of the MICROSOFT WINDOWS family (made by Microsoft Corporation of Redmond, Washington) and that includes a Web browser, such as MICROSOFT INTERNET EXPLORER, NETSCAPE NAVIGATOR (made by Netscape Corporation, Mountain View, California), having a Java Virtual Machine (JVM) and support for application plug-ins or helper applications. A client may also be a notebook computer, a handheld computing device (e.g., a PDA), an Internet appliance, a telephone, an electronic reader device, or any other such device connectable to the computer network.

[77] The server can be any entity, such as the workstation 10, a computer platform, an adjunct to a computer or platform, or any component thereof, such as a program that can respond to requests from a client. Of course, a "client" can be broadly construed to mean one who requests or gets the file, and "server" can be broadly construed to be the entity that sends or forwards the file. The server also may include a display supporting a graphical user interface (GUI) for management and administration, and an Application Programming Interface (API) that provides extensions to enable application developers to extend and/or customize the core functionality thereof through software programs including Common Gateway Interface (CGI) programs, plug-ins, servlets, active server pages, server side include (SSI) functions and the like.

[78] In addition, software embodying at least some aspects of the invention, in one embodiment, resides in an application running on the workstation 10. In at least one embodiment, the present invention is embodied in a computer-readable program medium usable with the general purpose computer system 10. In at least one embodiment, the present invention is embodied in a data structure stored on a computer or a computer-readable program medium. In addition, in one embodiment, an embodiment of the invention is embodied in a transmission medium, such as one or more carrier wave signals transmitted between the computer system 10 and another entity, such as another computer system, a server, a wireless network, etc. The invention also, in at least one embodiment, is embodied in an application programming interface (API) or a user interface. In addition, the invention, in at least one embodiment, can be embodied in a data structure.

[79] Note that the system 10 of FIG. 1 is not limited for use with workstations. Some or all of the system 10 can, of course, be used for various types of processing taking place in the systems

described herein, as will be appreciated by those skilled in the art. Further, in at least some embodiments, a plurality of systems 10 can be arranged as a parallel computing system.

[80] As used herein, the Internet refers at least to the worldwide collection of networks and gateways that use the transmission control protocol/Internet protocol (TCP/IP) suite of protocols to communicate with one another. The World Wide Web (WWW) refers at least to the total set of inter-linked hypertext documents residing on hypertext transport protocol (HTTP) servers all around the world. As used herein, the WWW also refers at least to documents accessed on secure servers, such as HTTP servers (HTTPS), which provide for encryption and transmission through a secure port. WWW documents, which may be referred to herein as web pages, can, for example, be written in hypertext markup language (HTML). As used herein, the term "web site" refers at least to one or more related HTML documents and associated files, scripts, and databases that may be presented by an HTTP or HTTPS server on the WWW. The term "web browser" refers at least to software that lets a user view HTML documents and access files and software related to those documents.

[81] It should be appreciated that any one or more of the elements illustrated in the following embodiments may be located remotely from any or all of the other elements, and that any of the elements of a given embodiment may, in fact, be part of another system altogether. For example, a database accessed by one or more of the elements of a given embodiment may be part of a database maintained by an organization entirely separate from the system of the invention.

[82] In addition, it should be understood that, for the following embodiments, although they are described in connection with a facial recognition system, the invention is not so limited. Many aspects of the invention are usable with other biometric technologies, including but not limited to fingerprint recognition systems, iris recognition systems, hand geometry systems, signature recognition systems, etc. We have found that at least some embodiments of the invention are especially advantageous for biometric application that utilize information that can be captured in an image.

[83] **<u>First Illustrative embodiment</u>**

[84] FIG. 2 is an illustrative block diagram of a system implemented in accordance with a first embodiment of the invention. Referring to FIG. 2, the following elements are provided.

[85] FIG. 2 is a block diagram of a first system 5 for biometric searching, in accordance with one embodiment of the invention. The system 5 includes a workstation 10 (such as the one described more fully in FIG. 1) which is capable of receiving inputs from a number of sources, including image and/or data capture systems 15, external data systems 17 (such as remote clients in communication with the workstation 10 and/or which conduct searches using the workstation 10, data acquisition devices such as scanners, palm top computers, etc.), manual inputs 19 (which can be provided locally or remotely via virtually any input device, such as a keyboard, mouse, scanner, etc.), and operator inputs 21 (e.g., voice commands, selections from a menu, etc.). In one embodiment, the workstation in this embodiment is programmed convert captured images and/or received data into templates usable by the facial recognition search system, 25 (described further below). However, those skilled in the art will appreciate that the function of converting captured data into biometric templates can, of course, be performed by a separate system (not shown). Biometric templates, after being created at (or otherwise inputted to) the workstation 10 can be added to the database of enrolled biometric templates 25.

[86] The system 5 also includes a biometric search system which in this embodiment includes a facial recognition search system 25. Of course, it will be appreciated that instead of a face recognition search system 25 as the biometric search system, the system 5 of FIG. 2 could instead use a search system that utilized a different biometric, e.g., fingerprint, iris, palm print, hand geometry, etc. In addition, we expressly contemplate that hybrid biometrics systems (systems that use more than one biometric) are also usable as a biometric search system; one such system is described in our patent application entitled "Systems and Methods for Recognition of Individuals Using Multiple Biometric Searches", serial no. 10/686,005, filed October 14, 2003, which is incorporated herein by reference. We also expressly contemplate that certain graphics processing programs, such as CyberExtruder, can be adapted to work with this and other embodiments of the invention.

[87] Referring again to FIG. 2, the facial recognition search system 25 includes a search engine capable of searching the database of previously enrolled biometric templates 35. In one embodiment, the facial recognition search system 25 is a facial recognition system employing a local features analysis (LFA) methodology, such as the FACE-IT facial recognition system available from Identix of Minnesota. Other facial recognition systems available from other vendors (e.g., Cognitec FaceVACS, Acsys, Imagis, Viisage, Eyematic, VisionSphere,

DreamMirth, C-VIS, etc.) are, of course, usable with at least some embodiments of the invention, as those skilled in the art will appreciate.

[88] The system 5 also includes a biometric template database 35 comprising previously enrolled biometric templates (e.g., templates adapted to work with the facial recognition search system 25) and a demographic database 37 comprising demographic information 37 associated with each respective biometric template in the biometric template database 25. For example, in one embodiment, the biometric template database 35 and demographic database 37 are associated with a plurality of records of individuals who have obtained an identification document (e.g., a driver's license) in a given jurisdiction. Either or both of the biometric template database 35 and demographic database 37 can be part of a database of official records (e.g., a database maintained by an issuer such as a department of state, department of motor vehicles, insurer, employer, etc.).

[89] Either or both of the biometric template database 25 and demographic database 37 also can be linked to (or part of) databases containing many different types of records, which can enable an user to "mine" the data and link to other information (this may be more advantageous in the web-server embodiment of FIG. 3). For example, an investigator could use selected aspects of an original probe to probe other databases, and/or use the matches as probes for more matches (as described in our patent application entitled "Systems and Methods for Recognition of Individuals Using Multiple Biometric Searches", serial no. 10/686,005, filed October 14, 2003), which is hereby incorporated by reference. The system 5 can use biometrics, such as faces or fingerprints, for the follow-up search, or it can other data, such as names, addresses and date-of-births, for the follow-up search. Effectively, the system 5 turns matches into probes for more matches, and cross-references the results. In addition, the system 5 could search other databases, such as those linked to the individual's social security number or phone number, and cross-reference these results.

[90] Our testing of embodiments of the invention using large (10 million or more images) databases of images has found that such recursive database searching and/or database mining has the potential for significant fraud detection. For example, we have found multiple people sharing one license number. We have also found that people tend to get several fake licenses in a few months. These are patterns that such further analysis can detect and track. In at least some embodiments of the invention, we link this type of data to itself (and even the employees of the issuing authority) to help determine and/or investigate collusion, such as that by criminals,

operators and/or administrators of the issuing authority, information technology (IT) operators, consultants, etc.

[91] Referring again to FIG. 2, in some embodiments, the system 5 further includes a search results database 23 for storing the results of searches conducted by the workstation 10. As those skilled in the art will appreciate, the search results database 23, biometric template database 35 and the demographic database 37 can be implemented using any type of memory device capable of storing data records or electrical signals representative of data and permitting the data records or electrical signals to be retrieved, including but not limited to semiconductor memory devices (e.g., RAM, ROM, EEPROM, EPROM, PROM, etc), flash memory, memory "sticks" (e.g., those manufactured by Sony), mass storage devices (e.g., optical disks, tapes, disks), floppy disk, a digital versatile disk (DVD), a compact disk (CD), RAID type memory systems, etc.

[92] In at least some embodiments, the system 5 includes an image/data capture system 15, which can be any system capable of acquiring images and/or data that can be used (whether directly or after conversion to a template) for biometric system. The particular elements of the image/data capture system 15 will, of course be dependent on the particular biometrics used. For example, signature pads may be used to acquire signatures of individuals, camera systems may be used to acquire particular types of images (e.g., facial images, iris images), retinal scanners may be used to acquire retinal scans, fingerprint scanning and capture devices may be used to capture fingerprint images, IR cameras can acquire thermogram images, etc. Those skilled in the art will readily understand what particular pieces of equipment may be required to capture or otherwise acquire a given piece of data or a given image.

[93] In an advantageous embodiment, the image/data capture system 15 can be implemented to automatically locate and capture biometric information in an image that it receives. For example, in one embodiment of the invention that implements a face recognition biometric, we utilize proprietary Find-A-Face™ software available from the assignee of the present invention (Digimarc Corporation of Burlington, MA). Find-A-Face™ software has the intelligence to automatically (without the need for any operator intervention):

(i) follow a multitude of instructions and extensive decision and judgment logic to reliably perform the difficult task of locating human faces (with their many variations) within captured digital data (a digital picture);

(ii) once the particular human face is found within the captured digital data, evaluate multiple aspects of the found human face in the image;

(iii) determine, based upon this face location and evaluation work, how the system should position the human face in the center of the digital image, adjust the gamma level of the image, and provide contrast, color correction and color calibration and other related adjustments and enhancements to the image; and

(iv) repeatedly and reliably implement these and other functions for the relatively large volume of image capture s associated with producing a large volume of identification documents

[94] In another advantageous embodiment, we have found that biometric templates created based on the data captured using the image/data capture system 15 can be further improved by utilizing of various methods to improve finding particular biometric features, such as eyes, which can further be used to improve the performance of biometric searches that use facial recognition. For example, in one embodiment we use systems and methods described in commonly assigned provisional patent applications no. 60/480,257, entitled "Systems and Methods for Detecting Skin, Eye Region, and Pupils" and/or "Detecting Skin, Eye Region, and Pupils in the Presence of Eyeglasses" (Application No. not yet assigned, Attorney Docket No. P0903D—Inventor Kyungtae Hwang), filed October 23, 2003, both of which are hereby incorporated by reference. In addition, as described further in this application (in connection with FIG. 16), in at least some embodiments we implement a system that improves facial recognition by improving the eye coordinate locations used by the templates.

[95] The systems and methods described in this patent application are, in one embodiment, implemented using a computer, such as the workstation 10 of FIG. 1.

[96] Referring again to FIG. 2, in at least some embodiments the workstation 10 can be in operable communication with an ID document production system 39, which can, for example, include a printer controller 27 that controls the printing of ID documents by an ID document printing system 29. The ID document production system 39 can, for example, be a CI or OTC type document production system (as described previously and also as described in commonly assigned U.S. patent application serial no. 10/325,434, entitled "Multiple Image Security Features for Identification Documents and Methods of Making Same", which is incorporated herein by reference). In at least some embodiments, the workstation 10 communicates with the ID document production system 39 to control whether or not a given ID document will be created (for issuance to an individual) based on the results of biometric searching.

[97] Note that FIG. 2 is a version of the invention implemented without use of a web server, whereas FIG. 3 (described further herein) is generally similar, but includes a web server as part of the interface between the rest of the system and the biometric searching subsystem. Those skilled in the art will appreciate that systems can, of course, be implemented that operate in some modes using a web server, and in some modes not using a web server.

[98] **Second Illustrative Embodiment**

[99] FIG. 3 is a block diagram of a system 50 for biometric searching in accordance with a second embodiment of the invention. Note that in the following discussion, all references to particular brands and/or suppliers (e.g., Digimarc, Visionics) are provided by way of illustration and example only and are not limiting. Those skilled in the art can appreciate that other products from other suppliers having equivalent functionality and/or features can, of course, be substituted.

[100] *System overview*

[101] In this embodiment, images in digital form are captured periodically (e.g., daily) by an issuing party, such as a DMV. The captured digital images are enrolled in a specialized Identification Fraud Prevention Program (IDFPP) facial recognition database which makes it possible to search the database and find matches using only pictures. Enrollment is a numerical process which reduces facial characteristics to a series of numbers called a template. The IDFPP manages the periodic (e.g., daily) batches of images which are enrolled and searched and also manages the presentation of results in a form convenient to the user.

[102] The production of a Driver's License (DL) or Identification (ID) document requires many processes involving various people and systems. The following summary (presented in the context of the issuance of a driver's license, for illustrative purpose only) summarizes some of the steps of such a process. Basically the production of a DL/ID consists of a session in which the applicant is present, and ends when the applicant leaves (with or without a document). In one example, the session starts with an applicant being greeted at the Intake station 62. This greeting process accumulates information on the applicant, and the DMV mainframe 64 participates in the accumulation of this information. Subsequently, the DMV mainframe 64 issues a request to the image capture station 66. This request causes the image capture workstation 66 to collect the relevant data (images, demographic data, etc.) of the applicant and to produce the appropriate

document on a special printer which prints the DL/ID documents. The printer can be present at the DMV (e.g., a so-called "over-the-counter" (OTC) system) or can be remotely located for later issuance to the applicant (e.g., a so-called "central issue" (CI) system, or in some combination of the two). The central image server ("CIS") 58 participates in the collection of image and demographic data, as needed. The CIS 58 also receives any new images which may be captured during a given session.

[103] In one embodiment, the DMV mainframe 64 communicates only once with the image capture Station 66. This communication is one-way from the mainframe 64 to the capture station 66. The communication takes the form of a print request stream containing the request and certain relevant data required by the capture station 66 to produce the required document. capture stations can comprise many different elements, but in at least one embodiment consists of a workstation (e.g., as in workstation 10 of FIG. 1), camera tower, signature capture device, and (if applicable) connections to a DL/ID printer as well and/or a paper printer (such as for printing so-called "temporary" ID documents). Images captured by the capture station 66 are "uploaded" to the CIS 58 over a computer network such as the DMV network. Although not illustrated in FIG. 3, a capture station can be located remotely and communicate images to the CIS 58 over the world wide web, via a wireless data link, etc.

[104] In the embodiment of FIG. 3, two general methods are used to help detect fraud. The first is a physical method, and the second is an investigative method. Physical verification involves features on the ID document itself, such as overt and/or covert security features (including but not limited to ultraviolet ink, optically variable ink, microprinting, holograms, etc., as are well understood by those skilled in the art). These features help to provide verification that the document was produced by an authorized issuer and not produced in a fraudulent manner.

[105] Investigative methods utilizes processes such software to assist in the biometric determination of fraud. Specifically, this method helps to detect whether the same individual is applying for several different identities. This method has two actions associated with it:

1. **Selection** of a list of "candidate images" (in the stored database of images) which might match the face of the applicant

2. **Verification** (by visual inspection) as to whether fraud is in fact being committed

[106] The first action (selection) can be purely based in software. Since each person's face remains the same (for example, in the case of driver's licenses, during those ages in which people are allowed to drive automobiles by themselves), a system which can compare the faces of all the people applying for a drivers license to all others who are applying (or have applied in the past) for a driver's license, would identify all faces that are the "same". Thus, if a single person keeps applying for driver's licenses under various assumed names, this method would be effective if it is applied consistently.

[107] Many DMVs have a large number of "legacy" images of those who are issued driver's licenses. For example, a state like Colorado may have approximately 9 million facial images stored over several years of use. The process of manually checking these images against each new applicant would be humanly impossible. Therefore, the IDFPP implemented by FIG. 3 helps to provide a reliable and automated way to check the identity of each new applicant against images that are already stored in the state's legacy of driver license images (note that it is preferable that the legacy images be digitized to facilitate conversion to templates). However, although the system of FIG. 3 can help to select a list of potential candidates, it may not determine decisively that fraud is being attempted. For example, the system of FIG. 3 may bring up an image of a person who is the biological twin of the probe image (a legitimate person who exists and looks exactly like the applicant). Thus, another level of intervention, such as review by a human user, can help to finalize a suspicion of fraud. Thus, the system 50 of FIG. 3 permits a human user to perform such "verification" steps

[108] The following description illustrates the various software modules, databases and processes needed to implement the Facial Recognition System (FRS) of FIG. 3 as part of the Fraud Prevention Program (IDFPP) of this embodiment of the invention.

[109] The system 50 of FIG. 3 includes a facial recognition search system 52 ("FRS 52"), a web server 54, an investigative workstation 56, a central image server 58 (including a facial recognition interface 6 0), an intake station 62, a mainframe 64, and a capture station 66. The investigative workstation 56, intake station 62, mainframe 64 each can be a workstation similar to the workstation 10 of FIG. 1. The capture station 66 can be similar to the image/data capture system 15 of FIG. 2.

[110] Referring again to FIG. 3, the facial recognition (FR) interface 60 is an interface used to provide necessary information for communications between the CIS 58 and the facial recognition

search system 52 ("FRS 52"). The details of operation of the FR interface 60 will, of course, depend on the particular facial recognition search engine used, and we anticipate that those skilled in the art will readily understand how to create and/or adapt an interface for communication between any two system elements. We also note that, depending on the system elements, an interface such as the FR interface 60 may or may not be necessary.

[111] The web server 54 can be any type of web server. In one embodiment, the web server 54 is a Covalent Web Server that includes an SQL server, an Identix Enterprise Server, an MSMQ Server, and various Digimarc applications.

[112] The facial recognition search system 52 ("FRS 52") is a system that stores a "mathematical equivalent" (often called a "Template") of each digital image that is in the CIS 58. As discussed further herein, the process of selecting a group (if one or more exists) of candidate images which "match" a given probe image, involves searching through all the template images stored by the FRS 52. This is also known as a one-to-many search.

[113] The central image server 58 ("CIS 58") is a server that stores all the digital images of all individuals whose image has been captured and who have been issued an identification document over a predetermined time period. The CIS 58 can be a database of images that have been captured at a given location (e.g., a DMV), but is not limited to those kinds of images. For example, the CIS 58 can consist of one or more databases stored by differing entities (e.g., governments, law enforcement agencies, other states, etc.). In this manner, the system of the invention can be used for inter-jurisdictional searching.

[114] In one embodiment, the CIS 58 is a relational database linked to a repository of image files, along with a software module that provides access to them called a Polaroid Central Image Management System (PCIMS) that manages the input and retrieval of the image data. Of course, any system capable of managing the input and retrieval of image data would be usable as an image management system, and the use here of a proprietary PCIMS system is not intended to be limiting. Thus, the CIS 58 stores images and provides for their later retrieval (via the web server 54, intake station 62, and the investigative workstation 56).

[115] In one embodiment the CIS 58 comprises a Sun 450 Solaris system that includes subsystems handling demographics and locations of personal object files (called "poff" files). Poff files have a file format that is designed to encapsulate all the data needed to process an

individual ID document, such as an ID card. All the data needed to print and handle the card will be included in the file. This permits this file to be shipped as an entity across a network where it can be printed, displayed or verified without need for additional information. The specific fields and their order in text area are not specified, there is a provision for a separate block of labels for the fields for display purposes. The format is suitable for encoding on 'smart cards' as well as transmission and printing of the records. More information about the POFF file format can be found in commonly assigned U.S. patent application no.10/325,434, entitled "Multiple Image Security Features For Identification Documents and Methods of Making Same", filed on December 18, 2002 and published as US 2003/0183695 A1 on October 2, 2003. The contents of this application are hereby incorporated by reference. Of course, it is not necessary for the invention that the POFF file format be used. Those skilled in the art will appreciate that many different file formats can be utilized to manage data for printing onto an identification document.

[116] In at least one embodiment, the CIS 58 performs one or more of the following functions::

- accepts (from the capture station 66) and stores a predetermined portion (e.g., all) information for cards which require identification fraud prevention (IDFPP) processing
- responds to the FRS 52 when required to do so, by providing a predetermined portion (e.g., ALL) images captured during the business day so that these images can be enrolled in the FR database
- responds to the FRS 52 when required to do so, by providing a predetermined portion (e.g., all) PROBE images captured during a specified business day so that these probe images can be processed by the FRS 52
- allows for changes in the status of IDFPP related information for stored images. For example, status designators can be assigned, such as "Pending Investigative Review", and "Void by Enforcement" (these designators are not, of course, limiting). The changes in status may be initiated from the FRS 52 , or Investigative Workstation 56, depending on various functions exercised by the FRS 52 and Investigative workstation 56
- operates such that any change to the IDFPP status of a record, which causes it to become a predetermined status (e.g., "Void by enforcement") causes a corresponding change to the document status, (e.g., where the status is marked as "void").
- supports identification of approved/suspected ID documents during a nightly (or other periodic) processing phase (in at least one embodiment, records are uploaded in a batch process for further investigation , but that is not limiting – processing can occur as each image is captured and/or enrolled, or at virtually any other time)

- produces a printed report of the daily expected number of identification documents which require IDFPP processing. If desired, this report can be sorted in any desired manner (e.g., by last name).

[117] Two of the functions of the FRS 52 that pertain to the CIS 58 are enrollment and searching. Enrollment is the addition of facial images to the FRS 52 from the CIS 58 and searching is the matching of a particular image against this image repository on the FRS 52. In one embodiment, the FRS 52 has read and write access to the database of the CIS 58 and read access to its image files. The database of the CIS 58 is used both to initiate the processing of records and to store the results of that processing. The Poff files are used for the images (e.g., portraits) they contain, as it is these portraits that assist during the investigations described herein. The PCIMS of the CIS 58 are arranged so that the records in the database can be marked for enrollment or searching.

[118] Addition of images, in one embodiment, occurs as part of an enrollment process. In one embodiment, images are periodically uploaded from the CIS 58 to the FRS 52. Advantageously, this can occur outside of normal operating hours of the issuing authority. These images are then converted into templates and stored (in a process called "enrollment") in the FRS 52. After these images are stored, the FRS 52 retrieves all the images which are marked as probe images. Then, each probe is used to perform a one-to-many search for a list of candidates which match that probe. For each probe which actually results in two or more matches (the probe is already in storage and will match itself), the corresponding data in the CIS 58 is marked as "Awaiting Verification". This concludes the selection operation. In at least one embodiment, all other images (other than the image of the probe itself) can be "candidates" that are searched. In at least one embodiment, the images being searched are classified in advance by some parameter (e.g., race, hair color, specific demographic data associated with the image, etc.) to improve the speed and/or accuracy of searching.

[119] An investigator can later retrieve all probe images which have been marked as "Awaiting Verification". In at least one embodiment, the investigator is provided with a predetermined ordered method for comparing the candidates with the probe image. The investigator will visually (and otherwise) determine if a given probe actually matches the candidates selected by the selection operation. If the investigator concludes that one or more candidate images are indeed the same as the probe image, the investigator will "reject" the probe image and also select and reject one or all of the candidate images. This will cause each image (probe and selected

candidates) to be marked as "Void by Enforcement" in the CIS database. In addition, all candidate images which were not rejected by the investigator have the "Awaiting Verification" marking removed from them.

[120] If the investigator concludes that none of the candidate images match the probe image, the investigator will "accept" the candidate image. This will cause the "Awaiting Verification" to be removed from the probe and all its related candidates. This may conclude the investigation/fraud detection/prevention activity, or further action may occur. For example, if an identification document had been issued to a candidate "instantly" (in, for example, an over-the-counter system) and it is later determined that the applicant may be committing fraud, law enforcement officials may be notified. In another example, if the system is a central issue type of system (where the identification document is provided to the applicant at a later time), and the investigation of an applicant raises concerns (applicant is not "accepted"), issuance of the identification document from the central issuing authority may be delayed or prevented until further investigation occurs. Many other outcomes are, of course, possible.

[121] In one embodiment, when the FRS 52 communicates with the CIS 58, it provides transaction data (e.g., data taken when an individual attempts to get an identification document—such as a driver's license—from an issuer—such as a DMV). The transaction data includes FRS 52 specific data. The PCIMS of the CIS 58 receives the data and stores data in the database and image files of the CIS 58. The transaction data includes an indicator signaling whether or not a search should be performed using data (e.g., a portrait) contained in the transaction data, and the PCIMS module of the CIS 58 sets a corresponding indicator in an FRS data table (in the CIS 58) based on the search indicator. Another indicator can also be set to trigger enrollment of the portrait in the FRS 52 database. The FRS 52 can then read these values and process the records accordingly.

[122] **Third Illustrative Embodiment**

[123] FIG. 4 is a block diagram of a first system for biometric searching 70, in accordance with a third embodiment of the invention. Note that elements of the system of FIG. 4 that have common names and/or functions to the systems of FIGs. 2 and 3 (e.g., "investigator workstation") can, in at least one embodiment, be implemented using the same hardware and/o software described previously, and these elements, in at least some embodiments, operate

similarly to their namesakes in FIGs. 2 and 3. Of course, the names provided here are not limiting.

[124] Referring again to FIG. 4, the first system for biometric searching 70 includes a photo validation system (PVS) 91 (also referred to herein as an identification fraud prevention system (IDFPP) 91) and a facial recognition search subsystem 52. The photo validation system 91 includes an investigator workstation 56, image/person server 72, an image/person database (DB) 74, a data entry workstation 76, a non template face data server 78, a non template face data database 80 (also called a face image database 80), a system administrator workstation 82, an optional adaptable application programming interface (API) 84, and an optional external alignment engine(s) 79. The facial recognition search subsystem 52 includes a message queue server 84, a face search server 86, a face alignment server 88, one or more alignment engines 90, one or more face image data (FID) file handlers 92, one or more search engines 94, and a face template database 96 (also referred to the FID database 96). Each of these elements is described further below.

[125] The first system for biometric searching 70 provides requisite utilities for system administration and maintenance, which are done via the system administrator workstation 82 (which can, for example, be a workstation similar to workstation 10 of FIG. 1). These utilities are tools, programs, and procedures that system administrators can use to maintain the database, software, and other system components. The utilities are not necessarily directly related to the match search or the enrollment processes, and the typical operator/investigator need not necessarily be required to know anything about them to use the system effectively. Examples of operations that the System Administrator Workstation can perform include:

[126] Initializing a face image database 80 and/or face template database 96: Process the existing set of face images at the time of initial system install (align all or a predetermined portion of existing face images in the face image database 80). Direct the alignment server 88 to create a face template for each existing face image.

[127] Update face image database 80 and/or face template database 96: Periodically add newly acquired images and direct the search engine 94 to create a record for each new face image. This can typically occur on a daily basis. An illustrative system is capable of acquiring 8000 new images per day, but this is not limiting.

[128] The image/subject database server 72 (also referred to as an Image/Person server 72) is a storage/retrieval system for face images and the related subject data. It is analogous to the CIS 58 (FIG. 3). It accesses a plurality of face images and the corresponding subject data for the face images. In one embodiment, the face images and corresponding subject data are stored in the Image/Person database (DB) 74. The number of face images can steadily increase as images are enrolled to the system, and the face recognition system can incorporate on a regular basis newly added image/subject records and can be designed to scale to a large number of images. For example, in one implementation, we have worked with databases of around 11 million images. We do not, however, limit our invention to image databases of this size, and we have been able to scale various embodiments of our invention to about 20-40 million images. We expressly contemplate that embodiments of our invention can be scaled and adapted to work with databases of images that are as large as desired.

[129] The system of FIG. 4 also includes utilities for system administration and maintenance. These are tools, programs, and procedures that system administrators can use to maintain and update the database, software and other system components. In this embodiment, the system administration utilities are not necessarily directly related to the facial match search, and the typical operator/investigator is not necessarily required to know anything about these utilities to use the system effectively.

[130] A user, such as an investigator/operator, controls the search process through the investigator workstation 56. In this embodiment, the investigator workstation 56 has a graphical user interface (GUI) with the ability to be customized to duplicate the "look and feel" of systems that already exist at customer sites with similar functionality. Advantageously, the investigator workstation is designed to be easy for an operator to use. Illustrative examples of the "look and feel", as well as the operation, of an exemplary operator workstation and an exemplary user interface are further described in connection with the screen shots of some embodiments of the invention that are provided herein. Note that although only a single investigator workstation 56 is illustrated in FIG. 4, systems implemented in accordance with the invention may contain one or more investigator workstations.

[131] The data entry workstation 76 (which can, for example, be a workstation similar to the workstation 10 of FIG. 1) is used to add, update and remove non face recognition data to the image/subject (also called image/person) database 74. In this embodiment, the functionality of the data entry workstation 76 is highly dependent on the customers' needs. For example, in one

embodiment, the capture of subject images can be integrated in the data entry workstation 76. In one embodiment, the printing of identification document also can be integrated into the data entry workstation 76 or coupled to the data entry workstation 76 (as in FIG. 2). In addition, we expressly contemplate that the capture station described in commonly assigned U.S. patent application no. 10/676,362, entitled "All In One Capture station for Creating Identification Documents", filed September 30, 2003, can be used with (or instead of) the data entry workstation 76, and the contents of this patent application are incorporated herein by reference. We also note that although only one data entry workstation is illustrated in FIG. 2, the system as implemented in accordance with the invention may contain one or more data entry workstations.

[132] The face alignment server 88 receives alignment requests from the workstation 82 via the message queue server 84, and distributes the alignment requests to the alignment engines 90, and returns the alignment success to the requesting workstation 82. Alignment, in the context of facial recognition searching, refers to locating selected elements (e.g., eyes) in an image, so that a corresponding biometric template can be created. Also, the alignment server 88 can read specific alignment requests (see the "AlignOnlyRequest in FIG. 4) from a face alignment request queue in the message queue server 84 . In at least one embodiment, the alignment service is scalable. For example, to be able to serve large numbers of alignments per day, the alignment server can distribute the alignment requests to one or many alignment engine(s) 90. The scaling of the alignment service is, in an illustrative embodiment, designed to correlate to the number of new facial images (e.g., 8000 images) that are acquired in a given time period (e.g., per day). To accommodate the need of investigators for on the spot alignment, in at least one embodiment, single alignment requests can be posted with a higher priority, so they get places at the top of the alignment queue.

[133] Note, also, that in at least some embodiments, the PVS 91 optionally can include (or be in communication with) one or more external alignment engines 79, each of which is capable of aligning an image. As will be explained further in connection with FIG. 16, using an external alignment engine 79 can enable the PVS 91 to send images to the facial recognition search system 52 already aligned (e.g., with a set of eye coordinates). As explained further in connection with FIG. 8, in one embodiment, if the facial recognition search system 52 receives an image that is already aligned, it does not itself align the image, but instead uses the alignment information provided to it by the PVS 91 to conduct its searching. In a further embodiment (relating to FIG. 16), the PVS 91 can use one or more external alignment engines 79 (instead of

or in addition to the alignment engines 90 of the facial recognition search system 52) to compute sets of eye coordinates, to apply one or more predetermined rules to determine which eye coordinates are likely to the most accurate.

[134] The message queue server 84 handles the face align request queue and contains the list of all alignment requests that have not yet been completely serviced. When the alignment server 88 begins its alignment cycle, it reads the alignment request at the top of the face align request queue in the message queue server 84.

[135] The alignment engine 90 receives an alignment request from the alignment server 88, creates the face template and other related data and stores it in the face database 96 (also called the FID Files 96). The alignment engine 90 can perform an automatic alignment procedure and return a success/failure result, or take manual alignment information (see FIG. 6B) to create the face template. In one embodiment, the alignment engine 90 performs only one alignment at a time, and can then return the result to the alignment server 88 . When there is a successful alignment, the alignment engine 90 optionally can send the face template and the other alignment information to the face database server 92 (e.g., FID file Handler 92) for storage in the face database (FID Files 96). Two forms of alignment request (automatic and manual) can be sent to the alignment engine 90. FIG. 6A is a flowchart of a method used for an automatic alignment request, and FIG. 6B is a flowchart of a method used for a manual alignment request. Each of these methods is described further below.

[136] The message queue server 84 maintains a request queue for the Face Search and contains the list of all search requests that have not yet been completely serviced. When the face search server 86 begins its search cycle, it can read the search request at the top of the search queue.

[137] As noted above, use of the adaptable API 85 is optional and is not required for all embodiments of the invention. In at least one embodiment, the photo validation system 91 communicates directly to a specific facial recognition search system (the Identix FACEit system) via the message queue server 84, using Microsoft Message Queue (MSMQ) protocol. This is illustrated in FIG. 4A. Referring to FIG. 5A, the facial recognition system 52 provided by Identix includes a subsystem of Identix Engines 95 (including, for example, the alignment engines 90 and search engines 94 of FIG. 4, along with associated file handlers, etc.), the message queue server 84, and a layer called DBEnterprise 89. DBEnterprise 89 is a layer added on top of the Visionics application to manage queue messages and finalize the search results.

[138] In this embodiment (which includes only the message queue server 84), enroll and identify modules in the photo validation system 91 constantly monitor the information in an SQL tracking database 93. The SQL tracking database 93 is a repository that tracks what information is eventually going to uploaded to the image repositories (e.g., the CIS 58 (FIG. 3) and/or the image/person database 74, face images database 80). When new enroll or identify request becomes available, the SQL tracking database 93 formats an MSMQ message and places it on the request queue of the message queue server 84. DBEnterprise 89 extracts each request message and in turn formats another message and places it on a queue for one or more of the engines in Identix Engine(s) 95 (or, optionally, in every engine's queue) for identify requests. The Identix Engine(s) 95 receiving the message then process the request and place the results in the specified response queue on the message queue server 84. Appropriate modules in the photo validation system 91 can extract the responses from these queues and then process the results.

[139] In one embodiment, the photo validation search system 91 includes an adaptable API 85. The adaptable API 85 is an optional feature that can enable the photo validation system 91 to communicate with one or more facial recognition search systems 52, each of which may have different interfaces. With the adaptable API 85, the photo validation system 91 can communicate with facial recognition search systems 52 from different vendors, so that the photo validation system 91 need not be specifically designed and configured to work with a system from just a single vendor. The photo validation system 91 communicates with the facial recognition search system 52 (which can, for example, be a third party system from a company such as Identix or Cognitec), to perform at least two operations for the first system for biometric searching 70:

[140] ENROLL

Analyzes a facial image and create a **template** describing the image characteristics like eye coordinates, facial characteristics, etc.

[141] IDENTIFY

Searches the database of previously enrolled images and create a template ID list of possible matches based on the number of matched images and the confidence level of the matched image.

[142] The adaptable API 85, in one embodiment, is configured to work in accordance with a Berkeley Sockets Network (BSNET). (The reader is presumed to be familiar with Berkeley Sockets Networks, and this technology is not explained here). The adaptable API 85 works with the PVS 91 to enroll and identify images using BSNET to interface to an external facial recognition system 52. FIG. 5B is a diagram showing the process flow that occurs between the

PVS 91 (client) and facial recognition system 52 (server), in accordance with one embodiment of the invention.

[143] The PVS 91 has a process running on it that periodically monitors predetermined tables in the tracking database 93 for new enrollment and/or identify requests. When a new request becomes available, the information is collected and a call to an extensible markup language (XML) encoder will create a string of tag/data/endtag elements. In at least one embodiment, BioAPI compliant XML format is used to be compliant with standards such as the BioAPI standards. This string is then passed to the server application along with the data size and the actual data in text format.

[144] On the server side, the receiving module sends an acknowledgement to the fact that a request is received. A unique request id links each request to a response. A RequestMgr on the server side decodes the XML data buffer and places each token into proper structure format used by the 3rd party application. The server then spawns a thread and passes the request structure to it. The spawned thread makes a 3rd party API call to process the request. At this point, the thread waits for the response. When a response becomes available, the process collects the data, makes a XML call to format the data and creates a response message. The response message is then send to a module called ResponseMgr (which is responsible for processing all requests generated by the server application). The response manager examines the response and based on the unique id of the original request, processes the results by populating the tracking database records and setting this step's completion flag.

[145] The process flow for this embodiment is shown in FIG. 5B. In at least one embodiment, enroll and identify processes use polling. In at least one embodiment, enroll and identify process can be triggered by virtually any mechanism, such as a database status change, or some other mechanism like launchPad, a 3rd party application.

[146] *Enroll Sending Process*

[147] In this embodiment, the enroll process is generally (but not always) triggered by the changes in database records stored in a location such as a CIS 58 (FIG. 3). When a new license is issued, a record is added to the CIS database and predetermined tables in the database (in one embodiment, these tables include facial recognition or other biometric information, POFF information, and demographic information)are populated with information related to the new

person. In addition, a status flag is set to ready, 'R'. In one embodiment (batch mode), these new records are accumulated until the predetermined time when images are batch processed (e.g., an end of the day process.)

[148] At the predetermined time, on the tracking database 93, a new daily schedule record is created in a predetermined table (e.g., a table called the frDailySchedule table). This is a new batch job. In this embodiment, each batch job can process up to 5000 enroll and/or search requests. This batch job triggers a backend process (which we call frsmain) to check the CIS database for records with the frstatus flag set to ready 'R' (in other words, to check for records that are ready to be searched against a set of previously enrolled images, whether enrolled to this system or some other system).

[149] If such records exist (i.e., records ready to be searched) , then, the backend process reads each record, up to predetermined maximum set in the batch record (currently 5000), accesses the records poff file indicated by poff_location, extracts the person's portrait image, sets the frstatus flag to 'R' and populates a queue that we call the frENROLLMENTQ of the tracking database. These new records in the enrollment table have status flag, 'VisionicsStatus', set to 'N' while the frsmain transferring all batch records. When all batch records are transferred, then, frsmain sets the 'VisionicsStatus' flag to 'R' for ready. In addition, each record gets a new unique 'PersonID' which is used by the 3rd party application as the template id.

[150] The enroll process polls the frENROLLMENTQ for ready records to be enrolled, or can be triggered by the stored procedure which sets the completion flags for the new records to ready 'R'.

[151] In one embodiment, the enroll process includes the following steps

i) read each ready record from the enrollment table,

ii) set the 'VisionicsStatus' flag to started 'S',

iii) get the image URL path from the database record,

iv) fill in the request structure,

vi) call XML encoder to encode the request structure,

vi) call bsnet send request with the above information, and

vii) process the acknowledgment.

[152] The unique request id, which can the same as the current person id, is a relevant data element in enrolling the image and receiving the results.

[153] *Enroll Receiving Process*

[154] This is a function call inside the ResponseMgr. The response manager will accept the arguments passed to it by the RequestMgr. The response message indicates align, enroll and/or a search request. If enroll, then, it calls 'pvsProcessEnrollResponse' module. This module reads the response, locates the record having the same unique id, and updates the record information, such as eye coordinates, alignment confidence level, and date time information. It also sets the 'VisionicsStatus' flag to done 'D', and moveToCIS to ready 'R'. This last flag allows the backend to update CIS with the new enrollment data.

[155] *Identify Sending Process*

[156] There are multiple ways that a record is ready for identification, such as

End of an enroll process for a batch job,

User initiated identify request, via GUI or programming interface

Through drill down (see our patent application entitled "Systems and Methods for Recognition of Individuals Using Multiple Biometric Searches", which is referenced and incorporated by reference elsewhere herein), and/or

Through operator using database table frPROBEQ status flags

[157] The identify request, similar to the enrollment request, examines the alignment information for the image being searched. If no alignment information available, it will make a call to the alignment module. The record will remain unchanged until the alignment information is available.

[158] When all information, including the image, the alignment information, maximum number of matched records, and maximum confidence level is known, a search request is formatted and XML encoded and sent to the server.

[159] *Identify Receive Process*

[160] This is a function call inside the ResponseMgr. The identify response includes a list of matched template IDs and each ID's confidence level. The identify response process makes a

database call to get the information for the record being searched. This includes whether this is a single search or a batch search and number of records requested with maximum threshold value.

[161] The single search is when an investigator initiates a search from a list of existing search candidates, or the investigator uses unique CIS record id to access the image, or search is done using an image file, or a drill down search. The batch search is result of a daily batch enroll and search process.

[162] The receive process updates the searched record with the number of matches returned, inserts a new record into the frCANDIDATES table with the records id (template id) and the confidence level, and sets the candidate flag to ready 'R'. The candidate records will be updated by the backend.

[163] The backend process reads each ready candidate record and using the record id extracts CIS information about the person, including location of the poff, demographics information, portrait image, finger print images, signature image, and updates the tracking database. When all candidates of a searched record are populated, the searched record becomes ready for viewing.

[164] *Ping process*

[165] This module is used to ping the server to make sure the server is up and listening for calls. Each module in this component can to make this call to make sure the server is up and running. If not, a message is logged and the process terminates.

[166] *Operation of System of FIG. 4*

[167] Referring again to FIGs. 4 and 5, the alignment server 88 begins an alignment by reading the alignment request from the Face Alignment Request queue in the message queue server 84. Batch alignment requests are handled by putting a portion of alignment requests on the alignment request queue. If the face image is part of the alignment request, it can be parsed out of the request (step 200 of FIG. 6A). For example, software (such as the previously described Find-A-Face, the previously described "pupil detection" patent applications, etc.) can be used to find a face and/or the eyes in the image (step 202). Specific software adapted to locate eyes in an image can be part of a facial recognition search engine 94. For example many facial recognition search engine vendors include eye finding as part of their offerings. We have found that, in at least one embodiment of the invention, the accuracy of facial searching can be improved by using

the eye finding of a first vendor (e.g., Cognitec) together with the facial recognition searching of a second vendor (e.g., Identix). In another embodiment, we have found it advantageous to use an inventive method for selecting the best eye location; this method is described more fully in connection with FIG. 16, herein.

[168] Referring again to FIG. 4, the face image and the related alignment settings are then sent to the next available alignment engine 90. The Face Alignment Server 88 waits for the alignment engine(s) 90 to return a result. The alignment engine 90 can return a result such as a success, failed or low confidence result together with the computed alignment information (eye positions). In at least one embodiment, to prevent results from being lost due to network failures, workstation crashes, etc., the results are not discarded until the requesting workstation acknowledges receiving the result.

[169] Referring again to FIG. 6A, based on the alignment information created for the face (step 204), a face template is created (step 206). If there is a failure in creating a face template (step 208) (for example, if the eyes were not located in the image), then an error message is returned (step 210). If there is no failure (e.g., if the returned result is success or low confidence), then the alignment information and face template are returned to the face data server 78 via the message queue server 84 (step 214). In one embodiment, we have found that an alignment engine 88 can performs an average of 30 alignments per minute. Scaling can, improve performance; for example, in one embodiment, to accommodate to higher performance needs, several alignment engines 90 are arranged serve one alignment server 88.

[170] Referring to FIG. 6B, for the manual alignment request, the image is parsed out of the alignment request (step 220), and alignment information (e.g., manually entered eye locations) are also parsed out of the alignment request. The manually entered eye locations can be selected manually by an operator viewing an image (e.g., by sliding lines or crosshairs on a screen and noting the respective x and y coordinates of the location of each eye.) The manually entered eye locations also can be selected via a combination of manual and automated functionality. For example, eye finding software can be used to find eye locations in an image and display tentative locations to a user (e.g., in the form of cross hairs, marks resembling the letter "X" at eye locations, circles or other shapes, etc.). The operator can then adjust the displayed eye coordinates as needed. The details of such a process are known and used in many different environments and are not necessary to explain her (for the reader to try an example of such a process, see the "try it on" feature at www.eyeglasses.com which locates a user's eyes in an

uploaded image, for the purpose of showing to the user how the user would look in a given pair of glasses).

[171] Based on the manually provided alignment information, the alignment server 88 attempts to create a face template (step 224). If there is a failure in creating a face template (step 228) (for example, if the eyes locations provided did not result in a valid template), then an error message is returned (step 230). If there is no failure (e.g., if the returned result is success or low confidence), then the alignment information and face template are returned to the face data server 78 via the message queue server 84 (step 232).

[172] Referring again to FIG. 4, the face search server 86 receives search requests from the investigator workstation 56, distributes the search to the search engines 94, collects and compiles the resulting match set, and returns the match set to the requesting investigator workstation 56. In one embodiment, the face database 96 is partitioned so that a given search engine 94 searches only its respective partition.

[173] The search engine 94 receives search requests from the search server 86 , executes the search on its partition of the face database 96 and returns the resulting match set to the search server 86. In one embodiment, we have found that the search cycle can execute at a minimum rate of about twenty million faces per minute, per search engine 86, but this rate is not, of course, limiting. To increase the speed of searching, in at least some embodiments the system 70 can use multiple search engines 86. For example, a configuration with 5 search engines can scale up to one half million faces per minute. We have found that in another embodiment of our invention, each search engine can search about 1.5 million faces.

[174] The FID (face image descriptor) File Handler 92 maintains the database of face templates 96, one for each face image intended as a candidate for matching. Note that in at least one embodiment of the invention, there can be more than one FID file handler 92. For example, in one embodiment of the invention, we have a FID file handler for each template used by a so-called "two pass" biometric system (which uses a so-called coarse biometric template followed by a so-called fine biometric template, e.g., a coarse template of about 84 bytes to do a "first pass" search of a database of other coarse templates, followed by a search of a portion of the "first pass" results using the "fine" template). The face template is a preprocessed representation of the face that a search engine can use in matching search. In at least one embodiment of the invention, the face template is a template usable with a so-called local feature analysis (LFA)

type of facial recognition algorithm, such as is used in the IDENTIX FACE IT product. Operation of at least part of this algorithm is detailed in U.S. patent No. 6111517, which is incorporated by reference in its entirety. The FID Handler 92 does not necessarily store the raw images (as discussed further below). The alignment engine 90 can generate the face templates. The initial face data set can be constructed at any time; in one embodiment, the initial face data set is constructed at the time of system installation. After the initial face data set is constructed, the administration workstation 82 can supply new images for which face data can be added to the FID Files. These new images can be provided periodically (e.g., daily or weekly), in response to a request, or upon the occurrence of a condition. This process is similar to the "enrollment" process of FIG. 3.

[175] To provide scalability and high performance, the face templates can be distributed over multiple computers. The FID File handler 92 is responsible for balancing the data load on multiple data servers. The FID File handler 92 provides a programming interface, so that the other components can retrieve the information they need to perform their tasks. The alignment engine(s) 90 can send face data records to the FID File handler 92 o be added to the face database 96. The FID File handler 92 is transparent to the alignment engine(s) 90 as to on which database partition the data can be stored. In this embodiment, data is added only through the alignment engine(s) 90.

[176] The FID Files 96 (also referred to as the face database 96) are the repositories for face templates. To achieve scalability they may be distributed over multiple computers. In this embodiment, each of search engines has its own set of FID Files 96 to minimize the I/O bottleneck when searching.

[177] The non template face data server 78 (also referred to herein as the misc. face data server 78) maintains the database of face template related data. In one embodiment, face template related data includes data other than the face template itself, such as name, address, biometric information (e.g., fingerprints), and alignment information. Each face template in the FID Files 96 has a respective entry in the misc. face database. In one embodiment, the misc. face data server 78 does not store the raw images. The alignment engine 90 generates the misc. face data. In this embodiment, the initial face data set is constructed at the time of system installation; it can be appreciated, however, that the initial face data set can be created at other times (e.g., before or after system installation). After the initial face data set is constructed, the administration

workstation periodically supplies new images for which misc. face data can be added to the database. New images for which misc. face data can be added can also be supplied.

[178] The misc. face database 80 (also referred to as the "Non Template Face Data 80") is a database of face template related data. This data includes alignment and reference information. In addition, it contains the lookup tables to describe the references between entries in the image/subject database and the FID Files 96.

[179] Operators/investigators can control the search process through use of the investigator workstation 56. In this embodiment, the investigator workstation is a personal computer (PC), but it will be appreciated that any device capable of running a browser (e.g., PDA, web-enabled phone, pocket PC, etc.) and displaying images is usable as a workstation, such as the technologies described for the workstation 10 of FIG. 1. In this embodiment, search transactions, made up of several simple, discrete steps, repeat continuously either automatically in batch mode, or asynchronously upon operator initiation. Each transaction generates a complete result set for each new probe image to search against.

[180] FIG. 7 is a flow chart of a method for conducting biometric searches at the search engine 94 of the system 70 of FIG. 4. The search engine 94 receives a search request (step 300) and the search engine loads the aligned probe image (step 302). The search engine 94 searches for matching templates that are stored on the database partition that is physically on the same machine as the search engine 94 (step 304). For each entry in the search list, the face template is retrieved from the face database (step 306), and it is matched against the probe face. A confidence score is created and stored for each of those matches (step 308). The finished array of search results is sent to the requesting face search server 86 (step 312) . A match result record consists of the face template identifier, the subject identifier and the match score.

[181] FIG. 8 is a flow chart of a method for conducting biometric searches at a user workstation, in accordance with one embodiment of the invention. The operator of the workstation 56 receives a search request (step 400). The search request can be delivered by any known means, including by paper document, by transportable media such as floppy disk, by computer network, or by other methods. The request can be a signal received by either the workstation itself or the operator. The operator can receive the request through one means (e.g., telephone call, oral request, message on a different workstation) and act on the request using the workstation.

[182] In one embodiment, the search request comes by listing one or more candidates to be investigated on a probe image verification list. FIG. 10 is an illustrative example of a screen shot of a probe image verification list, in accordance with one embodiment of the invention. An investigator selects one or more records on the list to verify.

[183] The request includes a probe image file, or a means to obtain it, e.g. information about the probe image file, a reference to an entry in the image/subject database, or any other information necessary to locate and/or obtain the probe image file. The probe image is a digitally stored image of a human face, against which the matching search can be conducted.

[184] The workstation 56 loads the probe image and text data associated with the request (step 402). If the face picture contained in the request is not available in a digitally stored form, in at least one embodiment, the means to create a digital image (e.g. scanner, etc.) can be used. For example, a scanner can be made available at the investigator workstation. The digital face image is loaded into the workstation software, and a Search Request Message is created. FIG. 9 is an illustrative example of a screen shot of a user interface showing an image that can be used as a probe image, in accordance with one embodiment of the invention.

[185] Probe images that are not stored in the image database do not necessarily contain any alignment information. For not previously aligned probe images (step 404), an alignment request is made to the alignment server 88 (step 404), which returns alignment information. This request can be executed at a high priority, so that the workstation operator can verify the result. If the automatic alignment fails, the workstation 56 can also provides a tool (not shown in FIG. 8 but described elsewhere herein, such as in FIG. 6B) for the operator to manually align the probe image

[186] The workstation operator specifies the face search settings, and other constraints for the search (step 406), then submits the request (which may include other information, such as search settings) to the Face Search Server 86 via the Message Queue Server 84 (step 408). For example, the workstation operator selects the query set on which the face match can be performed. She/he also selects a minimum threshold and/or a maximum number of returned matches. Other advanced settings can be specified by the administrator on a per face database basis.

[187] The Face Search Server 86 reads the Search Request from the message queue, distributes the request to the search engine(s) 412, and returns the match set to the workstation (steps 424).

[188] Upon submitting the search request to the message queue server, the operator sets a priority for the request. The message queue server maintains a search request queue for the Face Search Server. This queue contains the list of search requests submitted by the workstation(s) that await service by the face search server. The workstation operator reviews the match set and conducts further processing as desired. The workstation handles in an appropriate manner any failed search requests.

[189] The face search server 86 begins a search by reading the search request from the search queue and parsing out the probe image (see, e.g., the method of FIG. 6A). Other information, such as alignment information, also may be parsed out. The face search server 86 also parses out the alignment information, and the query set to be searched on. The following steps are performed, in accordance with one embodiment of the invention:

[190] Handling a Face Search Request

[191] - The face search server 86 builds the list of face templates that can be searched from the selection chosen by the investigator

- The search template list and the probe record with the alignment information are sent/distributed to the search engine(s) 94
- The face search server 86 waits for the search engine(s) 94 to return a resulting match set then builds a combined match set
- If the search request is hierarchical (has several stages with different recognition settings) the face search server 86 selects a subset of the match set, and re-send/distribute it to the search engine(s) 94
- Finally, the combined match set is send to the requesting workstation 56.

[192] To prevent results from being lost due to network failures, workstation crashes, etc. the message queue server 84 stores a Search Result (named, in this illustrative embodiment, "SearchResult") until it is discarded by the workstation.

[193] A match set can contain a sorted array of identifiers for the face data and the subject data. Records in the match set can have a relative match score ("face score" that indicates the determined level of similarity between the image probe and the database images. FIGs. 11A and 11B are illustrative examples of probe images 100, 101 and returned results 102 through 116, respectively, for the system of any one of FIGs. 2-4, and FIG. 13 is an illustrative example of a

screen shot of a candidate list screen presented to a user, in accordance with one embodiment of the invention. As these figures illustrate, an investigator can readily compare a probe image with one or more candidate matches, both visually and based on relative match score

[194] Note that, to minimize overall use of system resources, and to separate image data from face data, the result set returned to workstations 56 by the Face Search Server 86 does not necessarily have to contain image data. Rather, in this embodiment, the match set can contain pointers, or other unique identifiers, to image data. The workstation 56 can use the pointers to retrieve the raw image data from the image database server. For example, in one embodiment, the match set does not necessarily contain face images. Rather, the match set contains identifiers for face images and subject data stored on the image/subject server. To display or otherwise process any images identified in the match set, the workstation first retrieves them from the image server

[195] After receiving the match result set from the face search server, the workstation operator may process images selected from the match set in any of the following ways:

- Display images for comparison to the probe image (see FIGs. 12 and 14)
- Print display images
- Display or print reports
- Obtain fingerprints of subjects identified by selected images (see FIGs. 12 and 15)
- Select an image from the match set and submit it as the probe image for a new search (processes for doing this are also described more fully in our "Systems and Methods for Recognition of Individuals Using Multiple Biometric Searches", serial no. 10/686,005, filed October 14, 2003

[196] Those skilled in the art can appreciated that other ways of processing images are, of course, possible.

[197] After locating matches, the investigator can flag a record as void, potentially fraudulent, etc. This designation can be associated with the image until removed, and the flag (or other notes to the image) can remain visible even if the record is retrieved again in a different search.

[198] **Fourth Illustrative Embodiment**

[199] *Database Partioning*

[200] In one embodiment, we have found that some database portioning techniques can improve the speed and/or accuracy of searching. These techniques can be advantageous for applications where there are a very large number of legacy images that are never deleted or replaced (e.g., as in many DMVs). For applications such as these, the database can be broken up in active an inactive (or "almost" inactive) parts. In some embodiments, after an image is enrolled (and a template is created) , all the information about the image (such as so-called Binary Large Object (BLOB) "Image BLOB") is essentially inactive. One no longer needs access to the image for searching purposes, only for displaying search results. Another way to think about activity is to say: in at least some situations, the actual images are needed only for enrollment and display and nothing else. After enrollment, images can technically be deleted from at least a portion of the database since they are not needed for searching, either (the searching is done using templates). In one embodiment, the images will only be displayed if they rank high enough on a given search. Thus, the architecture of the search engine 94, file handler 92, search server 86, and/or face database 96 can be modified to separate the basic functions that require speed (enrollment, identification and verification) and those that don't (e.g., the user interface).

[201] We have found several ways to accomplish this portioning. In the first embodiment, the image BLOBS are kept in the face database 96, but they put are in a separate, indexed table on separate physical disk unit, in contiguous disk blocks. A foreign key in the new BLOB table ties it to the existing tables. Note that the particular server being used may dictate whether such control over space allocation is possible (e.g., SQL Server may not allow this level of control over space allocation, but Oracle does). In addition, in at least one embodiment, we distribute the blob image database on the nodes. After successful enrollment (enrollment is described further herein), images can be "archived" on a database stored on each node. One advantage is that each database can be limited (at least today) to about 1 million records. Once the database is "full" no more images will be added to it. This may make backup and recovery an easier job, although care may need to be taken because all the enrollment activity is now directed to one or two "active" nodes.

[202] In a second embodiment, image BLOBS are removed from the database. This can be accomplished using, for example, Oracle's BFILE data type, which may give efficiencies by reducing the database size, but keeps the benefits of using a recognized SQL data type.

[203] In a third embodiment, we leave images in the file system and store only a path to them. We have found this to be a workable approach. We have also evolved to a file structure based on the date that is very helpful when examining lots of records. It also avoids problems that develop with UNIX when the number of files in a directory grows beyond 40,000. One example of a structure that we have used is:

\volume name\YYYY\MM\DD\<filenames> or

\volume name\YYYY\DDD\<filenames>

[204] Some advantages of this embodiment include:

- It easy to convert a path from Unix to Windows format
- The number of records on any given day doesn't stress the operating system
- It is easy to logically group files for backup media

[205] In a fourth embodiment, we cache the face image records (FIRs). In this manner, a node could store all the FIRs allocated to it in a large file on the node itself. Loading it into memory will be far faster than reading rows from a database. This may affect the operation of dynamic partitioning, which can be rectified at least partially by adding another column to the images table to indicate that a node is full and the partition is no longer available for updates.

[206] **Fifth Illustrative Embodiment**

[207] The fifth illustrative embodiment of the invention applies some of the previously described systems, methods, user interfaces, and screen shots to provide an ID fraud prevention system optimized for use with DMVs, together with methods and processes for interacting with the ID fraud prevention system, including a user-friendly user interface, for searching a database of images for a match to a probe image. The features of this embodiment may be especially useful for large databases of images.

[208] *Overview of the Verification Process*

[209] In this embodiment, verification is the process of discovering DMV customers who have used false documents to obtain more than one license. The ID Fraud Prevention system of this embodiment assists the DMV investigator searching for multiple identities on documents issued by an issuing authority, such as a DMV. In the normal course of the issuance process, a DMV

customer presents documentation to establish his or her identity. In most cases, the DMV has no certain way to determine if the customer's identity is false.

[210] *Finding fraudulent customer records*

[211] The Fraud Prevention Program is used to quickly and automatically find those customers who already have one or more "valid" driver's licenses. Images uploaded daily from branch offices are sent to the DMVs Fraud Prevention system. The customer's portrait is enrolled (encoded for searching) and permanently stored in the special database used for performing searches and comparisons.

[212] After all images are enrolled, licenses tagged by the DMV as "new issuances" are automatically compared to the entire library of photos on file to see if a match or a close match exists. In one embodiment, the library of photos on file can be over 10 million images. The library of photos advantageously is kept current every day except for a very small percentage of images that fail for one reason or another.

[213] After the database is searched for matching images, one of two results may occur.

1. No match may be found: If no image in the Fraud Prevention database resembles the new photo, it is checked off in the Central Image Database as "passed by the system". This means that the likelihood of match to any one picture is so low that it is not worth reporting it, or having n investigator look at it. This is the result one would normally expect when a customer who is new to the DMV is getting a license for the first time

2. Possible matches are found: This outcome requires an investigator to look at the customer's photo and the possible matches found in the IDFPP database. It is up to the investigator to determine if photos are in fact a match and if so, what to do with the information. It is important to remember that the Fraud Prevention software is providing the user with its best assessment and *not* positive proof.

[214] Terminology

[215] The following words have a special meaning in the context of fraud prevention in this embodiment of the invention:

Browser	Microsoft Internet Explorer version 6.0 or higher

Candidate	A customer record returned by the IDFPP search process. A candidate is rated with a *confidence level*
Candidate List	A list of candidate images found by the IDFPP software to be similar to the probe image. All the candidates are organized so they can be viewed together with the probe image.
Confidence Level	This is number from 0 to 100 assigned to each image in the candidate list. A value of 100 means that the candidate should match the probe image. A value of zero mean it totally unlike the probe image.
Duplicate	A candidate image that is obviously the same as the probe image is loosely referred to as a duplicate. A duplicate image may be in the database as a result of operator error, computer error or fraud.
Fraud	This term applies to duplicate records (licenses) present in the DMV database that are the result of a deliberate attempt to conceal or alter the customer's identity. A duplicate is determined after all other possible sources have been eliminated such as operator or computer error. Fraud is **not** determined by the IDFPP system. A DMV investigator needs to make this determination, and in most cases will need supporting information from other sources.
Identical	Images are said to be identical if an image was inserted into the Central Image Server twice. This is usually the result of operator or computer error. If found by the IDFPP software, an image identical to the probe will be assigned a confidence level of 99 or 100. This is not a case of fraud.
List Size	This term refers to the size of the candidate list which appears on the verification screen. Typically, the list size

	is set to 15 or 25 images.
Match	This term is used loosely to mean a duplicate record was found.
Probe	This is the image used when searching for possible matches. Typically, it is the picture of a DMV customer who is getting a license for the very first time.
Progressive Search	If an investigator finds one or more interesting candidate images, he may use the candidate URNs to initiate a single search. A search with a candidate image may yield more matches to the original probe image.
Single search	A single search selects an image from the Central Image Server and uses it as probe to search IDFPP for possible matches.
Threshold	As each candidate record is obtained fro the IDFPP search database, the confidence level is compared to a system-wide value. If the candidate is above the threshold, it remains on the candidate list. If it is below the threshold, it is not added to the list.
Timeout	When an investigator stops moving the mouse or clicking on buttons, a count down timer started. The timer is initialized to the timeout value. When it gets to zero, the user is logged off. The timeout value is typically set to 5 minutes, but the system administrator may change this value.
Verification	This is the process of examining probe and candidate images to verify the absence of fraud. Probe images are verified automatically by the system if all the candidate images are below the confidence level threshold. Probe images that have candidate records above the threshold can be verified by an investigator.

[216] Batch Processing of Enrolled Images

[217] In this embodiment, newly captured images from (from one or more image capture locations, such as branch DMV offices) are periodically uploaded to the Central Image Server (CIS). For example, in a DMV application, newly capture images are uploaded to a DMV CIS after the close of business each day.

[218] Also, the library of enrolled images is searched with images tagged as new issuances. The results of this search are available in the morning for an investigator to review. In at least one embodiment, the search begins only after the batch of newly captured images is enrolled. This procedure increases that the chance that a DMV customer will be caught if he is shopping for multiple licenses on a single day. Verification lists can be generated that one or more images were found in the fraud detection system that were similar to the probe images. If no matches were found, a verification list is not generated.

[219] System Requirements:

[220] The IDFPP (ID Fraud Prevention Program) database and verification software of this embodiment can be accessed with any browser capable of browsing the Internet. In one embodiment, the IDFPP is accessible using Microsoft's Internet Explorer 6.0 (or later). The browser can, for example, be resident on a personal computer running the WINDOWS operating system and this version of Internet Explorer.

[221] However, those skilled in the art will appreciate that virtually any-other web-enabled devices (e.g., personal digital assistants (PDA's), laptops, mobile phones, tablet computers, etc.) capable of communicating with a display screen (whether built in or not) and/or an input device, are capable of being used in accordance with the invention. Thus, for example, remote users (e.g., law enforcement personnel) may be able to remotely access the network of the invention and determine "on the fly" whether a given identification document, such as a license, may have been fraudulently obtained. For example, the remote user could use a portable scanning device capable of capturing a digitized image to scan a drivers license image, then conduct a search of the IDFPP system to further investigate possible fraud relating to the image and/or the holder of the drivers license.

[222] The device running the browser should be capable of connecting to or communicating with the DMV network (depending, of course, on the network setup). To logon to the DMV

network and/or IDFPP system, a given user may need certain access privileges. If required, an IDFPP database administrator can set up a user's username and password to use with IDFPP. Note that the username and password need not be the same as those used for DMV network access. In one embodiment, the administrator of the IDFPP database system can setup the IDFPP database permissions which with varying access levels, such as "Junior" or "Senior" permissions.

[223] Once these items are set up, a user is ready to logon and start verifying images. This process begins, in one embodiment, by entering a predetermined URL in the browser's address field. The URL brings the user to the IDFPP logon screen.

[224] After logging on, a user can spend a significant portion of time viewing either the verification list (e.g., FIG. 10) or the gallery of candidates presented on the verification screen (e.g., FIGs. 11 and 13). Advantageously, the user interface of this embodiment is designed so that progress through the screens moves in a "straight line" with very little branching to keep things simple. In this embodiment, because it is important to finish work on each screen, even if a user cancels, the screens do not include a browser "Back" button. In cases where it is necessary to make this choice, an explicit back button is provided. If a user finds a candidate image of interest and wants to perform a new search using the candidate as a probe (e.g., the progressive searching described previously), the user can use a so-called "cut and paste" feature (e.g., such as the cut and paste features available in WINDOWS and the MAC OS) to copy the URN associated with the image into a single search input field.

[225] **Sixth Illustrative Embodiment**

[226] In our sixth illustrative embodiment of the invention, we have found that we can improve the accuracy and/or usability of facial recognition search engines, such as those used in the embodiment described herein, by improving the accuracy of the eye locating (alignment step), to improve the accuracy of the template based on the eye locations.

[227] Many known face recognition systems, for example, occasionally fail to correctly find the subject's eye location. In addition, inexactness can result because algorithms create a "probe" template from a digitized portrait and then search the entire database of templates for "near matches" instead of exact matches. This process results in a list of candidate matches which are ranked in order of likelihood. For certain images the face recognition software recognizes that is has not properly located the eyes and does not generate a face recognition template (e.g., the

alignment failures described previously herein). For other particular images, incorrect eye location is not detected and an invalid template is produced. It would be desirable to detect and possibly correct invalid templates as images provided either by a capture station or a legacy database are enrolled into a template database.

[228] We have found that commercially available facial recognition software does not meet the requirements of some types of customers, such as DMV customers. Vendors have created software that is directed at surveillance applications, but from a DMV perspective this software can have serious limitations. For example, vendor software that we have evaluated has some or all of these features:

- Optimized for databases of less than 1 million records or less
- Designed to have a human evaluate each image capture d and assist the program when it is enrolling the image in a search database
- Designed to take advantage of multiple image capture s of the same individual
- Designed to compare new images to a short "watch list" and present an operator with immediate feedback.

[229] All of these features, except possibly the "watch list" , can be a limitation in DMV applications for at least the following reasons:

- DMV image databases range in size from a few million to 80 million records and grow every day since DMVs typically do not delete any customer images, even those of deceased license holders
- Duplicate images are created at the license renewal cycle and it is rare to see more than 2 images of the same person in today's databases
- Enrollment of existing "legacy" database preferably occurs automatically and cannot require operator intervention.

[230] At least some conventional face recognition algorithms include an initial processing step to locate the eyes of a subject in an image of the subject's face. After the eyes are located a template engine provides a template by processing the face image. For example, at least some facial recognition software available from vendors perform portrait enrollment in roughly two steps:

[231] First, after some conventional image enhancement, a Cartesian coordinate system is established on the portrait by locating the centers of each eye. The line formed by the centers is one axis and the midpoint between the eyes is locates the second, perpendicular axis.

[232] After the coordinate system is established, the manufacturers' proprietary algorithms extract other facial features that are useful when matching one face with another. The features are encoded into a short binary template and added to a database of templates. In practice, the template database is keyed to information, such as a name and address so it is possible to identify an individual if the portrait matches one in the database.

[233] Each step in the above process entails levels of imprecision. We have noted that step 2 – the matching of templates depends heavily on the "quality" of the template created during step 1. If the digitized portrait used to create the template is subjectively a high quality portrait and the probe image used later in a search is also high quality, then the first image is nearly always found. The manufacturers give some guidance on this point and at least some recommend that:

- The optical axis of the camera lens should be perpendicular to the plane of the face to within 15 degrees;
- The portrait should be taken at a scale so that at least 100 pixels are between the centers of the eyes;
- The subject should have his eyes open and should not be looking up or down;
- The "probe" images used in a search should be taken under the same lighting conditions (color temperature, contrast, substantially without shadows) as the those in the template database.

[234] If these conditions are not met, the algorithms are likely to fail at step 1 and not create a template. For example, in most cases, no template is created if the subject's eyes are closed. This is reported by the vendor's software in about 1% of the images we tested.

[235] However, when a "good" portrait is captured, the algorithms still may fail to locate the position of the eyes correctly. Our studies have shown that the algorithms fail this way in about 7% to 20% of the images. When this type of failure occurs, the vendor's algorithms create a template but do not report an error. Incorrect templates are created which will almost never match another photo of the same individual. Failure to find eyes properly can result from many different factors, including whether or not an individual is wearing glasses or jewelry, hair style, whether subject is wearing a hat, how shiny the subject's skin is, etc.

[236] This unreported failure (creation of an incorrect template) effectively "deletes" the image from the template database by making it a non-participant. For databases containing more than 10,000 images, it is impractical to correct these failures by viewing every image in the database and manually correcting the eye coordinates. This is an unacceptably high error rate for many of such customers.

[237] In a first example of one of our tests, we obtained a sample of 300 images from a state's DMV database and enrolled them with software from two different facial recognition vendors (Imagis and Identix). The eye coordinates produced by each algorithm were verified manually and incorrect locations were noted. We ran searches on a small number of portraits that were incorrectly enrolled and verified that we could not match other images of the same individual (a second, slightly different portrait). After manually correcting the coordinates, we ran searches again and verified that matching software succeeded. Based on this testing, we discovered that different subsets of portraits were contained in the set of resulting "failures" and that by combining this information we can reduce the total number of failures (that is, increase the accuracy).

[238] In this embodiment, we provide methods for potentially detecting and/or correcting incorrect eye location. In one aspect of this embodiment, we correct eye location by means of additional eye location algorithms when used in conjunction with legacy database images and a combination of additional eye location algorithms, manual eye location under operator control, or image recapture when the face images are generated by an identification capture station. Advantageously, at least some embodiments of this aspect of the invention may provide increased face recognition accuracy by building a more accurate template database from legacy images and captured images, which will provide more accurate templates.

[239] FIG. 16 is a flow chart of a method for improving the accuracy of facial recognition searching, in accordance with one embodiment of the invention. An image of the subject is received (step 1200). The image can be captured at a capture station or, in at least one embodiment, can be an already-enrolled legacy image. If required for eye finding by a particular algorithm, pre-processing steps can occur to prepare the image for finding eyes, such as removing extraneous information (e.g., background) from the image (step 1202), finding a head, face, and/or skin in the image (step 1204), and resizing, centering, and/or the image if needed (step 1206). Then, the eyes of the subject are found in the image (step 1208).

[240] This step can use multiple eye location modules/engines in parallel (e.g., facial recognition engines 1 through N, which each may have an eye finding functionality) (steps 1218, 1220, 1222) to process the image, return eye coordinates (step 1209). Generally, each eye locating module returns (X,Y) eye location coordinates. Optionally, the eye locating module can also return an indication of success or failure of the eye location process. In at least some embodiments of the invention, the step of finding eyes in the image (step 1208) can be accomplished using on or more of the following:

- Process the image with primary face recognition module which returns a failure indicator and eye location coordinates
- Process image with a "blob" feature detector module configured to find eyes in a scaled centered image
- Process image with a secondary face recognition module to obtain eye location coordinates
- Process image with a third party proprietary face recognition algorithm which locates a eyes in an identification image

[241] The evaluation of the eye coordinates (step 1210) can be automated, manual, or a combination of automation and manual. Automated evaluation can involve one or more rules (described further below) which are applied to the coordinates. Evaluation (automated or manual) also can include one or more of the following types of analysis of the returned eye coordinates.

[242] Consistency checks: determine that both eyes are not in the same place, determine that horizontal and/or vertical eye locations are realistic.

[243] Statistical comparisons: compare eye location coordinates provided by each eye finding module, check tolerances between modules, compute average coordinate values, variance etc., which can help to eliminate anomalous coordinates, smooth errors, etc.

[244] General analysis: Check for other predetermined potential template problems based on eye location coordinates

[245] Evaluation provides a success or fail indication as well as eye location coordinates to be used by the template engine. If it is determined that there is a problem with the primary face

recognition module's eye location coordinates and the problem can be corrected, updated eye location coordinates (based on the correction) are provided from one of the other modules.

[246] Evaluation also can involve application of a predetermined rule to evaluate and determine the "final" eye coordinates (step 1210). We have found that various rules can be used on one or more of the returned sets of coordinates, assuming that at least some of them are "acceptable" (step 1214). A determination of whether results are "acceptable" can involve many different factors. For example, if a one or more of the eye locating modules did not find eye coordinates at all, and it is still possible to get a new image of the subject, the image of the subject may be automatically or manually recaptured (step 1216) and the image is re-evaluated to locate new eye coordinates. If the eye coordinates returned by the eye locating modules are so different that no pair of coordinates for an eye is within some predetermined distance (e.g., 1 inch) at least one other set of coordinates, the results may be deemed to be unacceptable. In another example, if an eye locating module returns one eye coordinate that appears to be in a significantly different vertical position on the face than the other (e.g., left eye being 4 inches higher than right eye), results may be deemed to be unacceptable. Similarly, it may be deemed unacceptable if the left and right eye are in the same spot, or are more than several inches apart. Those skilled in the art will, of course, appreciate that many other patterns of returned results can be deemed to be not "acceptable".

[247] For example, in one embodiment we provide a "majority rules" type of implementation, where the coordinates are selected that are closest to (or an average of) those selected by a majority of the eye locating modules. For example, assume that for a subject image, 5 different eye locating modules returned the following X and Y coordinates for a right eye (only one eye is used here, for simplicity, but it will be appreciated that the returned coordinates for the left eye can be similarly evaluated, and, indeed, coordinates for both eyes can be evaluated at the same time). Table 1 shows the results:

[248] Table 1

Eye_Locating_Module	X Coordinate	Y Coordinate
Vendor A	55	110
Vendor B	35	90
Vendor C	52	100
Vendor D	58	115
Vendor #	21	21

[249] As table 1 shows, the results from Vendors A, C, and D are closest to each other and in the "majority". In one embodiment, the eye coordinates can be assumed to be the average of these majority results, which would result in an assumption that the X coordinate has a value of 55 and the Y coordinate has a value of 108. These "averaged" locations can be used as the eye location.

[250] The above is just one illustrative example of a rule that can be used to select the "best" eye coordinates from the returned eye coordinates. Other rules that we have tested and which may be usable include any one or more of the following:

- Determining a broad area of interest for the location of both eyes and rejecting points outside of the area.
- Applying a weighted voting mechanism to the results from each of the results generated by the different eye locating modules (blob detection), and picking the one with the highest weighted number of "votes". Historical accuracy data can be used to assist in computing weights (for example a given eye locating module may be especially accurate for individuals with darker skin but less accurate for individuals with lighter skin and that information can be noted by the operator prior to finding the eyes, so that results from that eye finding module are weighted more heavily than those from other modules).
- Replacing the eye coordinate with the center of gravity of all the candidate locations
- Excluding points that are too far away from the frame midline after the captured image is scaled and framed.
- Excluding point outside of boundaries for each possible eye location
- Rejecting points if the location is not contained in a blob with the correct "eye"

characteristics.

- Rejecting pairs of points if the slope of the connecting line is too high (or too low) (e.g., the results show one eye has a markedly different vertical location than the other)

[251] Referring again to FIG. 16, if the automatic eye location (using the eye locating modules) fails after processing a predetermined number of images (step 1214), then the capture station operator is prompted (if the image is being enrolled) to manually set eye locations (step 1224 and 1226). The remaining steps (creation of template, etc.) are similar to those described in connection with other figures herein, and are not repeated here.

[252] *Testing*

[253] We used a set of 300 DMV images (the same DMV images which we used in the "first example" described above) as input to an industrial vision system manufactured by Acuity Corp. This algorithm uses a technique know as "blob detection" that decomposes an image into areas that meet certain programmed conditions. Geometric features of interest for each blob are then measured and stored in a database. The features we used to sort the blobs were:

[254] eccentricity – measuring roundness

[255] total area (in pixels)

[256] length and orientation of the major axis

[257] length and orientation of the minor axis

[258] (X,Y) coordinates of the centroid

[259] We removed all the blobs that had a Y coordinate that could not be paired with another blob (to within a narrow tolerance band). We also removed blobs that were outside an area of interest (a band of pixels just below the top of the head).

[260] Blobs that had at least one companion at about the same height were checked to see if the X coordinates spanned the midline of the picture frame. All blobs that did not have a companion in the other half of the frame were eliminated.

[261] Finally the remaining blobs were checked according to size and eccentricity. Those that were roughly the same size and similar orientation, were paired.

[262] Examining the results manually, we found that this approach could be used to provide a set of candidate eye coordinates in most cases.

[263] *Modifications to the Method of FIG. 16.*

[264] Additional steps can be added to the method of FIG. 16, if desired. For example, in one embodiment, if there are known duplicates of a subject (e.g., previous image capture s known to be of the same individual) already in the database, the newly generated template can be compared to the previous ones to determine if they match. If they do not, the operator can be given feedback to adjust the eye coordinates of the newly captured image.

[265] In one embodiment, even if the coordinates returned by the eye locating modules are deemed acceptable, the operator can override them and manually enter the eye coordinates. The operator also can manually override the threshold of step 1214 to retake further images of the subject (which can be advantageous if the subject accidentally moves or blinks during image capture).

[266] The method of FIG. 16 can be adapted to enroll images from a legacy database of images (e.g., where there is not the ability to re-capture images of the subject as needed). In one embodiment, multiple images can be processed if the legacy database includes multiple images for each person in the database. Manual eye location for legacy images is, of course, possible; however the number of images which require may manual correction can make this process impracticable.

[267] In at least one embodiment of legacy enrollment, if it is determined by the evaluator that the eye location is unacceptable and manual correction is not enabled, then no template is generated, and an indication of eye location failure is placed in the database.

[268] ***Additional Features of these and Other embodiments of the Invention***

[269] The embodiments of the invention disclosed herein, including the records of the investigations and searches, can be used in many ways, especially in ways that benefit law enforcement and/or other government entities. For example, data associated with multiple attempts at fraud by a given individual can be sorted by the geographic location (e.g., DMV

location) at which the individual sought the identification document (e.g., the location where an individual presented fraudulent credentials and/or had his/her image capture d). The list of locations may help law enforcement officials to determine patterns of attempted fraud, DMV locations where the most (and least) fraud occur, and possible geographic regions where an individual suspected of fraud may reside.

[270] In addition, the lists of fraudulent images may be useful as "watch lists" to be provided to other governmental and/or law enforcement agencies. Such "watch lists" could be compared to other lists, such as FBI "most wanted" lists, international terrorist watch lists, Immigration and Naturalization Service (INS) watch lists, etc., to attempt to track down the locations of individuals of interest. The batch processing features of at least some embodiments of the invention can also be utilized to assist other agencies and can be adapted to work with databases used by other systems. For example, in addition to comparing a given captured image to the database of images stored by the issuing agency (e.g., DMV), the given capture image also could be compared with one or more watch lists of images that are maintained by other agencies. The same features of the invention (detailed previously in the first, second, and third embodiments) can be used to search these other databases. Indeed, it should be appreciated and understood that the invention is applicable not just to issuers of identification documents (such as DMVs), but to virtually any agency or organization where it is important to locate any and all individuals who may match a given image.

[271] Furthermore, although the invention has heretofore been described using captured images, the invention can readily be implemented using so-called "live" images (e.g., live feeds from surveillance cameras).

[272] In addition, although the systems and methods described herein have been described in connection with facial recognition techniques and fraud prevention, the embodiments of the invention have application with virtually any other biometric technologies that lends itself to automated searching (e.g., retinal scanning, fingerprint recognition, hand geometry, signature analysis, voiceprint analysis, and the like), including applications other than fraud prevention. For example, the systems and user interfaces of the present invention could be used with a fingerprint recognition system and associated search engine, where an investigator is searching a fingerprint database for a match to a latent fingerprint image retrieved from a crime scene.

[273] Embodiments of the invention may be particularly usable in reducing fraud in systems used for creating and manufacturing identification cards, such as driver's licenses manufacturing systems. Such systems are described, for example, in U.S. Patent Nos. 4995081, 4879747, 5380695, 5579694, 4330350, 4773677, 5923380, 4992353, 480551, 4701040, 4572634, 4516845, 4428997, 5075769, 5157424, and 4653775. The contents of these patents are hereby incorporated by reference.

[274] Such card systems may include a variety of built in security features, as well, to help reduce identity fraud. In an illustrative embodiment of the invention, the biometric authentication process described above can be used during the production of a photo-identification document that includes a digital watermark. Digital watermarking is a process for modifying physical or electronic media to embed a machine-readable code therein. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. The code may be embedded, e.g., in a photograph, text, graphic, image, substrate or laminate texture, and/or a background pattern or tint of the photo-identification document. The code can even be conveyed through ultraviolet or infrared inks and dyes.

[275] Digital watermarking systems typically have two primary components: an encoder that embeds the digital watermark in a host media signal, and a decoder that detects and reads the embedded digital watermark from a signal suspected of containing a digital watermark. The encoder embeds a digital watermark by altering a host media signal. To illustrate, if the host media signal includes a photograph, the digital watermark can be embedded in the photograph, and the embedded photograph can be printed on a photo-identification document. The decoding component analyzes a suspect signal to detect whether a digital watermark is present. In applications where the digital watermark encodes information (e.g., a unique identifier), the decoding component extracts this information from the detected digital watermark.

[276] Several particular digital watermarking techniques have been developed. The reader is presumed to be familiar with the literature in this field. Particular techniques for embedding and detecting imperceptible watermarks in media are detailed, e.g., in Digimarc's co-pending U.S. Patent Application No. 09/503,881 and U.S. Patent Application No. 6,122,403. Techniques for embedding digital watermarks in identification documents are even further detailed, e.g., in Digimarc's co-pending U.S. Patent Application Nos. 10/094,593, filed March 6, 2002, and

10/170,223, filed June 10, 2002, co-pending U.S. Provisional Patent Application No. 60/358,321, filed February 19, 2002, and U.S. Patent No. 5,841,886.

[277] Concluding Remarks

[278] In describing the embodiments of the invention illustrated in the figures, specific terminology (e.g., language, phrases, product brands names, etc.) is used for the sake of clarity. These names are provided by way of example only and are not limiting. The invention is not limited to the specific terminology so selected, and each specific term at least includes all grammatical, literal, scientific, technical, and functional equivalents, as well as anything else that operates in a similar manner to accomplish a similar purpose. Furthermore, in the illustrations, Figures, and text, specific names may be given to specific features, modules, tables, software modules, objects, data structures, servers, etc. Such terminology used herein, however, is for the purpose of description and not limitation.

[279] Although the invention has been described and pictured in a preferred form with a certain degree of particularity, it is understood that the present disclosure of the preferred form, has been made only by way of example, and that numerous changes in the details of construction and combination and arrangement of parts may be made without departing from the spirit and scope of the invention . In the Figures of this application, in some instances, a plurality of system elements or method steps may be shown as illustrative of a particular system element, and a single system element or method step may be shown as illustrative of a plurality of a particular systems elements or method steps. It should be understood that showing a plurality of a particular element or step is not intended to imply that a system or method implemented in accordance with the invention must comprise more than one of that element or step, nor is it intended by illustrating a single element or step that the invention is limited to embodiments having only a single one of that respective elements or steps. In addition, the total number of elements or steps shown for a particular system element or method is not intended to be limiting; those skilled in the art can recognize that the number of a particular system element or method steps can, in some instances, be selected to accommodate the particular user needs.

[280] It also should be noted that the previous illustrations of screen shots, together with the accompanying descriptions, are provided by way of example only and are not limiting. Those skilled in the art can recognize that many different designs of interfaces, screen shots, navigation patterns, and the like, are within the spirit and scope of the invention.

[281] Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms, and in many different environments. The technology disclosed herein can be used in combination with other technologies. Also, instead of ID documents, the inventive techniques can be employed with product tags, product packaging, labels, business cards, bags, charts, smart cards, maps, labels, etc., etc. The term ID document is broadly defined herein to include these tags, maps, labels, packaging, cards, etc.

[282] It should be appreciated that the methods described above as well as the methods for implementing and embedding digital watermarks, can be carried out on a general-purpose computer. These methods can, of course, be implemented using software, hardware, or a combination of hardware and software. Systems and methods in accordance with the invention can be implemented using any type of general purpose computer system, such as a personal computer (PC), laptop computer, server, workstation, personal digital assistant (PDA), mobile communications device, interconnected group of general purpose computers, and the like, running any one of a variety of operating systems. We note that some image-handling software, such as Adobe's PrintShop, as well as image-adaptive software such as LEADTOOLS (which provide a library of image-processing functions and which is available from LEAD Technologies, Inc., of Charlotte, North Carolina) can be used to facilitate these methods, including steps such as providing enhanced contrast, converting from a color image to a monochromatic image, thickening of an edge, dithering, registration, manually adjusting a shadow, etc. Computer executable software embodying the steps, or a subset of the steps, can be stored on a computer readable media, such as a diskette, removable media, DVD, CD, hard drive, electronic memory circuit, etc.).

[283] Moreover, those of ordinary skill in the art will appreciate that the embodiments of the invention described herein can be modified to accommodate and/or comply with changes and improvements in the applicable technology and standards referred to herein. Variations, modifications, and other implementations of what is described herein can occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed.

[284] The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in

this and the referenced patents/applications are also expressly contemplated. As those skilled in the art will recognize, variations, modifications, and other implementations of what is described herein can occur to those of ordinary skill in the art without departing from the spirit and the scope of the invention as claimed. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention's scope is defined in the following claims and the equivalents thereto.

[285] Having described the preferred embodiments of the invention, it will now become apparent to one of ordinary skill in the art that other embodiments incorporating their concepts may be used. These embodiments should not be limited to the disclosed embodiments, but rather should be limited only by the spirit and scope of the appended claims.